GUTRIDE SAFIER LLP
Seth A. Safier (State Bar No. 197427)
seth@gutridesafier.com
Marie A. McCrary (State Bar No. 262670)
marie@gutridesafier.com
Todd Kennedy (State Bar No. 250267)
todd@gutridesafier.com
Kali R. Backer (State Bar No. 342492)
kali@gutridesafier.com
100 Pine Street, Suite 1250
San Francisco, CA 94111
Telephone: (415) 639-9090
Facsimile: (415) 449-6469

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

VISHAL SHAH, JONATHAN GABRIELLI, and CHRISTINE Q. WILEY, as individuals, on behalf of themselves, the general public, and those similarly situated,

Plaintiffs,

v.

HILTON WORLDWIDE HOLDINGS INC.,

Defendant.

CASE NO.

CLASS ACTION COMPLAINT FOR INVASION OF PRIVACY; INTRUSION UPON SECLUSION; WIRETAPPING IN VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT (CALIFORNIA PENAL CODE § 631); USE OF A PEN REGISTER IN VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT (CALIFORNIA PENAL CODE § 638.51); COMMON LAW FRAUD, DECEIT AND/OR MISREPRESENTATION; UNJUST ENRICHMENT; BREACH OF CONTRACT; BREACH OF IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING; AND TRESPASS TO CHATTELS

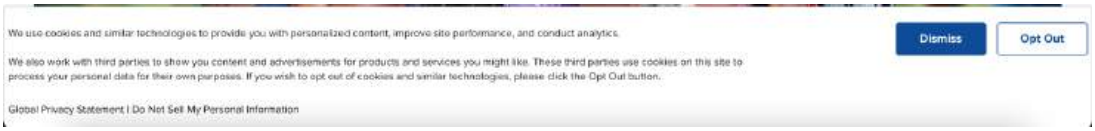
JURY TRIAL DEMANDED

TABLE OF CONTENTS

Plaintiffs Vishal Shah, Jonathan Gabrielli, and Christine Wiley ("Plaintiffs") bring this action on behalf of themselves, the general public, and all others similarly situated against Hilton Worldwide Holdings Inc. ("Defendant" or "Hilton"). Plaintiffs' allegations against Defendant are based upon information and belief and upon investigation of Plaintiffs' counsel, except for allegations specifically pertaining to Plaintiffs, which are based upon Plaintiffs' personal knowledge.

INTRODUCTION

1. This Class Action Complaint concerns an egregious privacy violation and total breach of consumer trust in violation of California law. When consumers visit Defendant's website (www.hilton.com, the "Website"), Defendant displays to them a popup cookie consent banner. Defendant's cookie banner discloses that the Website uses cookies but expressly gives users the option to control how they are tracked and how their personal data is used. Defendant assures visitors that they can choose to "Opt Out" of cookies as shown in the following screenshot:



2. Like most websites, Defendant designed the Website to include resources and programming scripts from third parties that enable those parties to place cookies and other similar tracking technologies on visitors' browsers and devices and to transmit cookies along with user data. However, unlike other websites, Defendant's Website offers consumers a choice to browse without being tracked, followed, and targeted by third party data brokers and advertisers. However, Defendant's promises are outright lies, designed to lull users into a false sense of security. Even after users elect to "Opt Out" of cookies, Defendant surreptitiously enables several third parties – including Google LLC (DoubleClick), Adobe Inc. (Adobe Marketing Cloud and Adobe Audience Manager), Microsoft, Inc. (Bing), Snap, Inc., *and more* (the "Third Parties") – to place and/or transmit cookies that track users' website browsing activities and eavesdrop on users' private communications on the Website.

3. Contrary to their express opt out or rejection of cookies and tracking technologies on the Website, Defendant nonetheless caused cookies, including the Third Parties' cookies, to be sent to Plaintiffs' and other visitors' browsers, stored on their devices, and transmitted to the Third Parties along with user data. These third-party cookies permitted the Third Parties to track and collect data in real time regarding Website visitors' behaviors and communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data.

4. The Third Parties analyze and aggregate this user data across websites and time for their own purposes and financial gain, including, creating consumer profiles containing detailed information about a consumer's behavior, preferences, and demographics; creating audience segments based on shared traits (such as millennials, tech enthusiasts, etc.); and performing targeted advertising and marketing analytics. Further, the Third Parties share user data and/or user profiles to unknown parties to further their financial gain.

5. This type of tracking and data sharing is exactly what the Website visitors who clicked or selected the "Opt Out" button on the Website's cookie consent banner sought to avoid. Defendant falsely told Website users that it respected their privacy and that they could avoid tracking and data sharing when they browsed the Website. Despite receiving notice of consumers' express declination of consent, Defendant defied it and violated state statutes, tort duties, and also breached its contractual duties and the implied covenant of good faith and fair dealing with Plaintiffs and those similarly situated Website users.

THE PARTIES

6. Plaintiff Vishal Shah is, and was at all relevant times, an individual and resident of San Jose, California. Plaintiff intends to remain in California and makes his permanent home there

7. Plaintiff Jonathan Gabrielli is, and was at all relevant times, an individual and resident of Oakland, California. Plaintiff intends to remain in California and makes his permanent home there.

8. Plaintiff Christine Wiley is, and was at all relevant times, an individual and resident of Long Beach, California. Plaintiff intends to remain in California and makes his permanent home there.

9. Defendant Hilton Worldwide Holdings Inc. is a Delaware corporation with its headquarters and principal place of business in McLean, Virginia.

JURISDICTION AND VENUE

10. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1332(d)(2). The aggregate amount in controversy exceeds $5,000,000, exclusive of interest and costs; and Plaintiffs and Defendant are citizens of different states.

11. The injuries, damages and/or harm upon which this action is based, occurred or arose out of activities engaged in by Defendant within, affecting, and emanating from, the State of California. Defendant regularly conducts and/or solicits business in, engages in other persistent courses of conduct in, and/or derives substantial revenue from products and services provided to persons in the State of California. Defendant has engaged, and continues to engage, in substantial and continuous business practices in the State of California.

12. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claims occurred in the state of California, including within this District.

13. Plaintiffs accordingly allege that jurisdiction and venue are proper in this Court.

SUBSTANTIVE ALLEGATIONS

A. Defendant Programmed the Website to Include Third-Party Resources that Utilize Cookie Trackers.

14. Every website, including the Website, is hosted by a server that sends and receives communications in the form of HTTP requests, such as "GET" or "POST" requests, to and from Internet users' browsers. For example, when a user clicks on a hyperlink on the

Website, the user's browser sends a "GET" request to the Website's server. The GET request tells the Website server what information is being requested (e.g., the URL of the webpage being requested) and instructs the Website's server to send the information back to the user (e.g., the content of the webpage being requested). When the Website server receives an HTTP request, it processes that request and sends back an HTTP response. The HTTP request includes the client's IP address so that the Website server to knows where to send the HTTP response.

15. An IP address (Internet Protocol address) is a unique numerical label assigned to each device connected to a network that uses the Internet Protocol for communication, typically expressed as four sets of numbers separated by periods (e.g., 192.168.123.132 for IPv4 addresses). IP addresses can identify the network a device is on and the specific device within that network. Public IP addresses used for internet-facing devices reveal geographical locations, such as country, city, or region, through IP geolocation databases.

16. Defendant voluntarily integrated "third-party resources" from the Third Parties into its Website programming. "Third-party resources" refer to tools, content or services provided by third-parties, such as analytics tools, advertising networks, or payment processors, that a website developer utilizes by embedding scripts, styles, media, or application programming interface (API) into the website's code. Defendant's use of the third-party resources on the Website is done so pursuant to agreements between Defendant and those Third Parties.

17. The Website causes users' devices to store and/or transmit both first-party and third-party tracking cookies. Cookies are small text files sent by a website server to a user's web browser and stored locally on the user's device. As described below, cookies generally contain a unique identifier which enables the website to recognize and differentiate individual users. Cookie files are sent back to the website server along with HTTP requests, enabling the website to identify the device making the requests, and to record a session showing how the user interacts with the website.

18. First-party cookies are those that are placed on the user's device directly by the web server with which the user is knowingly communicating (in this case, the Website's server). First-party cookies are used to track users when they repeatedly visit the same website.

19. A third-party cookie is set by a third-party domain/webserver (e.g., www.google.com; doubleclick.net; bing.com; tr.snapchat.com; etc.). When the user's browser loads a webpage (such as a webpage of the Website) containing embedded third-party resources, the third-parties' programming scripts typically determine whether the third-party cookies are already stored on the user's device and cause the user's browser to store those cookies on the device if they do not yet exist. Third-party cookies include an identifier that allows the third-party to recognize and differentiate individual users across websites (including the Website) and across multiple browsing sessions.

20. As described further below, the third-party cookies stored on and/or loaded from users' devices when they interact with the Website are transmitted to those third parties, enabling them to surreptitiously track in real time and collect Website users' personal information, such as their browsing activities and private communications with Defendant, including the following:

- **Browsing History**: Information about the webpages a Website user visits, including the URLs, titles, and keywords associated with the webpages viewed, time spent on each page, and navigation patterns;
- **Visit History**: Information about the frequency and total number of visits to the Website;
- **Website Interactions:** Data on which links, buttons, or ads on the Website that a user clicks;
- **User Input Data**: The information the user entered into the Website's form fields, including search queries, the user's name, age, gender, email address, location, and/or payment information;
- **Demographic Information**: Inferences about age, gender, and location based on browsing habits and interactions with Website content;

- **Interests and Preferences**: Insights into user interests based on the types of Website content viewed, products searched for, or topics engaged with;
- **Shopping Behavior**: Information about the Website products viewed or added to shopping carts;
- **Device Information**: Details about the Website user's device, such as the type of device (mobile, tablet, desktop), operating system, and browser type;
- **Referring URL**: Information about the website that referred the user to the Website;
- **Session Information**: Details about the user's current Website browsing session, including the exact date and time of the user's session, the session duration and actions taken on the Website during that session;
- **User Identifiers**: A unique ID that is used to recognize and track a specific Website user across different websites over time; and/or
- **Geolocation Data**: General location information based on the Website user's IP address or GPS data, if accessible.

(Collectively, the browsing activities and private communications listed in the bullet points above shall be referred to herein as "Private Communications").

21. Third-party cookies can be used for a variety of purposes, including (i) analytics (e.g., tracking and analyzing visitor behavior, user engagement, and effectiveness of marketing campaigns); (ii) personalization (e.g., remembering a user's browsing history and purchase preferences to enable product recommendations); (iii) advertising/targeting (e.g., delivering targeted advertisements based on the user's consumer profile (i.e., an aggregated profile of the user's behavior, preferences, and demographics); and (iv) social media integration (e.g., enabling sharing of users' activities with social media platforms). Ultimately, third-party cookies are utilized to boost website performance and revenue through the collection, utilization, and dissemination of user data.

22. Defendant is a globally recognized hospitality company and one of the largest and most well-known hotel chains in the world. Defendant operates a wide range of hotels and resorts under various brands, catering to different customer segments and needs. Defendant also owns and operates the Website, which allows visitors to receive information about hotels and make hotel reservations. As they interact with the Website (e.g., by entering data into forms, clicking on links, and making selections), Website users communicate Private Communications to Defendant, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data.

23. Defendant chose to install or integrate its Website with resources from the Third Parties that, among other things, use cookies. Thus, when consumers visit the Website, both first-party cookies and third-party cookies are placed on their devices and/or transmitted. This is caused by software code that Defendant incorporates into its Website, or that Defendant causes to be loaded. Because Defendant controls the software code of its Website, it has complete control over whether first-party and third-party cookies are placed on its users' devices and/or transmitted to third parties.

24. Defendant explained the third-party cookies it used on the Website as follows in its Privacy Statement:

> [We have collected the following categories of personal information in the past 12 months:]
>
> Internet or other electronic network activity information, including information regarding a customer's interaction with Hilton websites, applications, or advertisements
>
> [We have obtained this personal information from the following sources:]
>
> Directly from consumers themselves via cookies, server logs, web beacons, tags, pixels, and other similar technologies
>
> [We collected this personal information for the following business or commercial purposes:]

- Perform analytics in order to provide guests with personalized offers and content
- Perform analytics to improve business operations
- Marketing
- Share that data with advertising networks who serve personalized advertisements
- Detect and prevent fraud

[We have shared this personal information with the following categories of third parties:]

- Advertising networks
- Analytics providers for our websites and mobile applications

…

We partner with certain third-party service providers to collect information to engage in analytics, auditing, research, and reporting. These third parties may use server logs, web beacons, tags, pixels, and similar technologies, and they may set and access cookies on your computer or other device.

…

We also partner with third parties to provide advertising services that are targeted based on your online activities across websites, mobile apps, and devices over time (commonly referred to as "interest-based advertising"). Our advertising partners may collect information about your activities on our Services on your current device and combine it with information about your activities on other websites, mobile apps, and devices. They may collect such information using server logs, cookies, web beacons, tags, pixels, mobile advertising IDs (such as Facebook cookies or Google's Advertising ID), cross-device linking, and similar technologies. For example, our advertising partners may use the fact that you visited our website to target advertising to you on other websites and mobile apps on your current device or on other devices you use. They may match your browsers or devices if you log into the same online service on multiple devices or if your devices share similar attributes that support an inference that they are used by the same person or household. This means that information about your activity on websites or apps on your current browser or device may be combined and used with information collected from your other browsers or devices.

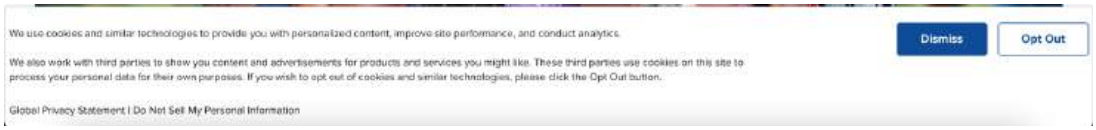
…

We also cooperate with third parties to serve targeted advertising based on your online activities across different websites, mobile applications, and devices over time. Our advertising partners may collect information about your activities related to our services on your current device and combine it with information about your activities on other websites, mobile applications, and devices. They may collect this information using server logs, cookies, web beacons, tags, pixels, mobile

advertising IDs, cross-device linking and similar technologies. This may include your personal information.[1]

B. Defendant Falsely Informed Users That They Could Opt Out of the Website's Use of Cookies.

25. When consumers in California visited the Website, the Website immediately displayed to them a popup cookie consent banner. As shown in the screenshot below, the cookie consent banner stated, "We use cookies and similar technologies to provide you with personalized content, improve site performance, and conduct analytics. We also work with third parties to show you content and advertisements for products and services you might like. These third parties use cookies on this site to process your personal data for their own purposes. If you wish to opt out of cookies and similar technologies, please click the Opt Out button." The banner then purported to provide users the opportunity to select an "Opt Out" of cookies button as shown in the following screenshot from the Website:



26. Website users who clicked or selected the "Opt Out" button, indicating their choice and/or agreement to opt out of or reject all cookies and tracking technologies in use on the Website, could then continue to browse the Website, and the popup cookie consent banner disappeared.

27. Defendant's popup cookie consent banner led Plaintiffs, and all those Website users similarly situated, to believe that they opted out of or rejected all cookies and tracking technologies, especially those that used to "personalize[] content, improve site performance, and conduct analytics" and those that allow third parties to "process your personal data for their own purposes." The banner further reasonably led Plaintiffs and those Website users similarly situated to believe that Defendant would not allow third parties, through cookies, to access their

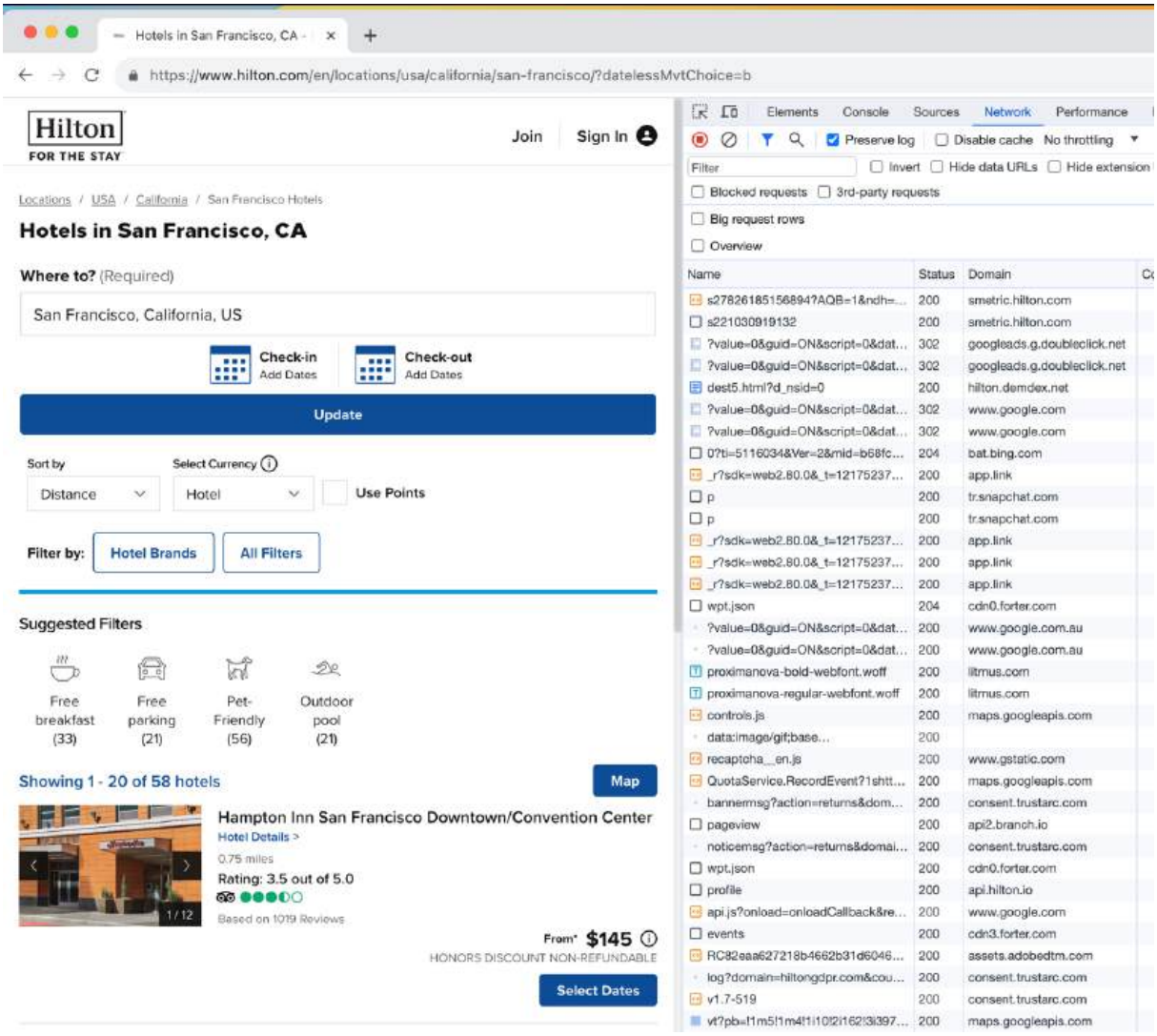
[1] Hilton's Global Privacy Statement (Last Updated: May 10, 2023) (available at https://web.archive.org/web/20231002094700/https://www.hilton.com/en/p/global-privacy-statement/) (the "Privacy Statement"). Defendant has subsequently updated its Privacy Statement but, based on information and belief, this version was in effect at the time that Plaintiffs opted out of cookies on the Website.

Private Communications with the Website, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data, upon clicking or selecting the "Opt Out" button.

28. Defendant's representations, however, were false. In truth, Defendant did not abide by its users' wishes. When users selected the "Opt Out" button, they provided notice to Defendant that they did not consent to the placement or transmission of third-party cookies that would allow those parties to obtain their Private Communications with the Website. Nevertheless, Defendant caused the Third Party tracking cookies to be placed on Website users' browsers and devices and/or transmitted to the Third Parties along with user data.

29. In particular, when users clicked or selected the "Opt Out" button, Defendant nonetheless continued to cause the Third Parties' cookies to be placed on users' devices and/or transmitted to the Third Parties along with user data, enabling them to collect user data in real time that discloses Website visitors' Private Communications, including browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data. In other words, even when consumers like Plaintiffs tried to protect their privacy by opting out of or rejecting cookies, Defendant failed to prevent cookies from being transmitted to Third Parties, enabling them to track user behavior and communications.

30. Some aspects of the operations of the Third Party cookies on the Website can be observed using specialized tools that log incoming and outgoing Website network transmissions. The following screenshot, obtained using one such tool, shows examples of Third-Party cookies being transmitted from a Website user's device and browser to Third Parties even after the user clicked the "Opt Out" button on the Website's popup cookie consent banner.



31. The screenshot above shows the "Network" tab of Chrome Developer Tools, which contains a list of HTTP network traffic transmissions between the user's browser and various third party websites while the user visited and interacted with Defendant's Website at https://www.hilton.com. The screenshot depicts only network traffic occurring ***after*** the user opted out of cookies using the cookie banner. As shown above, despite the user's rejection of all cookies by opting out, the user's interactions with the Website resulted in the user's browser making a large number of GET and POST HTTP requests to third party web domains like www.google.com; doubleclick.net; bing.com; tr.snapchat.com; etc., and others. As further shown in the right-hand column of the screenshot, the user's browser sent cookies along with those HTTP requests to the third parties.

32. This screenshot demonstrates that the Website caused third-party cookie data and users' Private Communications to be transmitted to Third Parties, even after consumers opted out of or rejected all cookies and tracking technologies by clicking or selecting the "Opt Out" button. All of these network calls are made to the Third Parties without the user's knowledge, and despite the user's rejection of all cookies.

33. Website users' Private Communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data, are surreptitiously obtained by the Third Parties via these cookies.

34. As users interact with the Website, even after clicking or selecting the "Opt Out" button, thereby opting out or rejecting the use of cookies and similar technologies for personalized content, advertising, and analytics, as well as the sale or sharing of the user's personal information with third parties for such functions, or other purposes, more data regarding users' behavior and communications are sent to third parties, alongside the cookie data. The third-party cookies that Defendant wrongfully allows to be stored on users' devices and browsers, and to be transmitted to the Third Parties, enable the Third Parties to track and collect data on users' behaviors and communications, including Private Communications, on the Website. Because third-party cookies enable Third Parties to track users' behavior across the Internet and across time, user data can be correlated and combined with other data sets to compile comprehensive user profiles that reflect consumers' behavior, preferences, and demographics (including psychological trends, predispositions, attitudes, intelligence, abilities, and aptitudes). These Third Parties monetize user profiles for advertising, sales, and marketing purposes to generate revenue and target advertising to Internet users. Advertisers can gain deep understanding of users' behavioral traits and characteristics and target those users with advertisements tailored to their consumer profiles and audience segments.

35. The Third Party code that the Website causes to be loaded and executed by the user's browser becomes a wiretap when it is executed because it enables the Third Parties—separate and distinct entities from the parties to the conversations—to use cookies to eavesdrop upon, record, extract data from, and analyze conversations to which they are not parties. When the Third Parties use their respective wiretaps on Website users' Private Communications, the wiretaps are not like tape recorders or "tools" used by one party to record the other. The Third Parties each have the capability to use the contents of conversations they collect through their respective wiretaps for their own purposes as described in more detail below.

C. Defendant's Conduct Violated Its Own Privacy Statement.

36. Defendant's aiding, agreeing with, employing, permitting, or otherwise enabling the Third Parties to track users' Private Communications on the Website using third-party cookies—even after those users click or select the "Opt Out" button—is particularly egregious given Defendant's additional written assurances in its Privacy Statement that users can, in fact, opt out of cookies and tracking technologies used on the Website. Specifically, Defendant represented to Plaintiffs and its users the following in the Privacy Statement:

> If you would like to opt out of the sale of your personal information, you may do so by clicking on the banner that appears on any Hilton website when you access that site from an IP address that relates to California or by visiting our website at datarights.hilton.com or click the "Personal Data Requests" link at the bottom of any Hilton website to submit your request. Please note that when you opt out of cookies, tags, and pixels, that opt out only pertains to the device and the browser that you are using when you opt out. If you wish to opt out for other devices or browsers, you must opt out again when you are using those devices or browsers.

Privacy Statement.

D. The Private Communications Collected As a Result of Third Party Cookies Transmitted When Visiting Defendant's Website.

1. Google Cookies

37. Defendant causes third party cookies to be transmitted to and from Website users' browsers and devices, even after users opt out of all cookies (including advertising and analytics cookies) to and from the **www.google.com** and **doubleclick.net** domains. These domains are associated with Google LLC's digital advertising and analytics platform that collects user information via cookies to assist Google in performing data collection, behavioral analysis, user retargeting, and analytics.[2] Google serves targeted ads to web users across Google's ad network, which spans millions of websites and apps. Nearly 20% of web traffic is tracked by Google's DoubleClick cookies.[3] Google's cookies help it track whether users complete specific actions after interacting with an ad (e.g., clicking a link or making a purchase) and provide analytic metrics that advertisers use to measure ad campaign performance. Further, by identifying users who have shown interest in certain products or content, Google's cookies enable its advertising platform to enable advertisers to show relevant ads to those users when they visit other websites within Google's ad network.[4]

38. Specifically, Google sends cookies when a web user visits a webpage that shows Google Marketing Platform advertising products and/or Google Ad Manager ads.[5] "Pages with Google Marketing Platform advertising products or Google Ad Manager ads include ad tags that instruct browsers to request ad content from [Google's] servers. When the server delivers the ad

[2] *See* Our advertising and measurement cookies (available at https://business.safety.google/adscookies/).

[3] *See, e.g.* https://www.ghostery.com/whotracksme/trackers/doubleclick.

[4] *See, e.g.* About cross-channel remarketing in Search Ads 360 (available at https://support.google.com/searchads/answer/7189623?hl=en); About dynamic remarketing for retail (available at https://support.google.com/google-ads/answer/6099158?hl=en&sjid=11962135750754589 08-NC).

[5] *See* How Google Marketing Platform advertising products and Google Ad Manager use cookies (available at https://support.google.com/searchads/answer/2839090?hl=en&sjid=11962135750754589 08-NC); *see also* Cookies and user identification (available at https://developers.google.com/tag-platform/security/concepts/cookies).

content, it also sends a cookie. But a page doesn't have to show Google Marketing Platform advertising products or Google Ad Manager ads for this to happen; it just needs to include Google Marketing Platform advertising products or Google Ad Manager ad tags, which might load a click tracker or impression pixel instead." *Id.* As Google explains, "Google Marketing Platform advertising products and Google Ad Manager send a cookie to the browser after any impression, click, or other activity that results in a call to our servers." *Id.*

39. Google also uses cookies in performing analytical functions. As Google explains, "Google Analytics is a platform that collects data from [] websites and apps to create reports that provide insights into [] business[es]."[6] "To measure a website … [one] add[s] a small piece of JavaScript measurement code to each page on [a] site." *Id.* Then, "[e]very time a user visits a webpage, the tracking code will collect … information about how that user interacted with the page." *Id.* Google Analytics enables website owners to "measure when someone loads a page, clicks a link, [ ] makes a purchase;" "completes a purchase"; "searches [] website or app"; "select content on [] website or app"; "views an item"; and "views their shopping cart."[7]

40. Google's cookies allow it to obtain and store at least the following user data: (i) browsing history, (ii) visit history, (iii) website interactions, (iv) user input data, (v) demographic information, (vi) interests and preferences, (vii) shopping behaviors, (viii) device information, (ix) referring URLs, (x) session information, (xi) user identifiers, and (xii) geolocation data.[8]

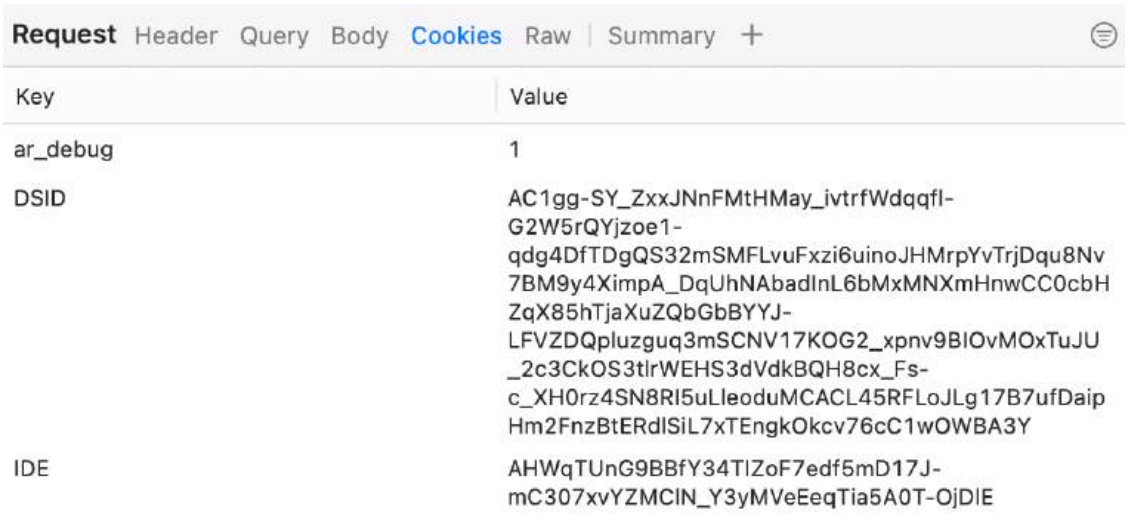
---

[6] How Google Analytics Works (available at https://support.google.com/analytics/answer/12159447?hl=en).

[7] Set up events (available at https://developers.google.com/analytics/devguides/collection/ga4/events); and Recommended events (available at https://developers.google.com/analytics/devguides/collection/ga4/events).

[8] *See* About the Google Tag (available at https://support.google.com/searchads/answer/7550511?hl=en); How Floodlight Recognizes Users (available at https://support.google.com/searchads/answer/2903014?hl=en); How Google Ads tracks website conversions (available at https://support.google.com/google-ads/answer/7521212); Google Ads Help, Cookie: Definition (available at https://support.google.com/google-ads/answer/2407785?hl=en); About demographic targeting in Google Ads (available at https://support.google.com/searchads/answer/7298581?hl=en&sjid=1196213575075458908-

41. For example, the Google software code that Defendant causes to be stored on and executed by the Website user's device causes the following cookie data to be sent to Google's domain, at https://googleads.g.doubleclick.net:



42. Google uses the "DSID" cookie to "identify a signed-in user on non-Google sites."[9] The "IDE" cookie is used "to personalize the ads [users] see" and "to show Google ads on non-Google sites."[10]

43. Further, along with all of this data, the Google software code that Defendant causes to be stored on and executed by the user's device causes the user's "user-agent" information to be sent to Google:

user-agent	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.0.0 Safari/537.36

NC&visit_id=638670675669576522-2267083756&ref_topic=7302618&rd=1); How Google Analytics Works (https://support.google.com/analytics/answer/12159447); Set up events (available at https://developers.google.com/analytics/devguides/collection/ga4/events); and Recommended events (available at https://support.google.com/analytics/answer/9267735).

[9] *See* https://policies.google.com/technologies/cookies?hl=en-US

[10] *See id.*

44. The "user-agent" corresponds to the device and browser that the user has used to access the Website. In this example, the user-agent value corresponds to Google's Chrome browser version 121, running on the Catalina version of macOS.[11]

45. Finally, the data sent to Google contains the user's IP address.

46. Because Google's cookies operate across multiple sites (i.e., cross-site tracking), the cookie enables Google to track users as they navigate from one site to another, and to comprehensively observe and evaluate user behavior online. Google's advertising platform aggregates user data to create consumer profiles containing detailed information about a consumer's behavior, preferences, and demographics and audience segments based on shared traits (such as females, Millennials, etc.), and to perform targeted advertising and marketing analytics.

47. Thus, the Google cookies used on the Website enable Google to track users' interactions with advertisements to help advertisers understand how users engage with ads across different websites. Further, the user data collected through the cookie enables the delivery of personalized ads based on user interests and behaviors. For instance, if a user frequently visits travel-related websites, Google will show her more travel-related advertisements. Further, the collected data is used to generate reports for advertisers, helping them assess the performance of their ad campaigns and make data-driven decisions (such as renaming their products). Further, Google's advertising platform enables advertisers to retarget marketing, which Google explains allows advertisers to "show previous visitors ads based on products or services they viewed on your website. With messages tailored to your audience, dynamic remarketing helps you build leads and sales by bringing previous visitors back to your website to complete what they started."[12]

48. Further, in its "Shared Data Under Measurement Controller-Controller Data Protection Terms," Google states: "Google can access and analyze the Analytics data customers

[11] There are many tools on the web that are capable of parsing user-agent strings to determine what browser and operating system they pertain to. One such tool is located at https://explore.whatismybrowser.com/useragents/parse.

[12] Dynamic remarketing for web setup guide (available at https://support.google.com/google-ads/answer/6077124).

share with us to better understand online behavior and trends, and improve our products and services—for example, to improve Google search results, detect and remove invalid advertising traffic in Google Ads, and test algorithms and build models that power services like Google Analytics Intelligence that apply machine-learning to surface suggestions and insights for customers based on their analytics data and like Google Ads that applies broad models to improve ads personalization and relevance. These capabilities are critical to the value of the products we deliver to customers today."[13] Thus, Google can have the capability to use the data it collects for understanding online behavior and trends, machine learning, and improving its own products and services.

2. Adobe Cookies

49. Defendant also causes third party cookies to be transmitted to and from Website users' browsers and devices, even after users elect to opt out of cookies, to and from the **demdex.net** and **omtrdc.net** domains. These domains are associated with Adobe Inc.'s Audience Manager, a data management platform, Adobe's Marketing Cloud, and Adobe's Experience Cloud Identity Service, a service which provides a universal, persistent ID to identify visitors across all Adobe products.

50. These cookies are used to assign a unique identifier to each site visitor, which enables Adobe to consistently recognize and track users across different sessions and domains (i.e., cross-site tracking) and collect and synchronize user data to comprehensively observe and evaluate user behavior online.[14] These cookies enable Adobe to obtain and store at least the following user data: (i) user identifier; (ii) website interactions; (iii) browsing history; (iv) visit history; (v) interests and preferences; and (vi) session information.[15]

---

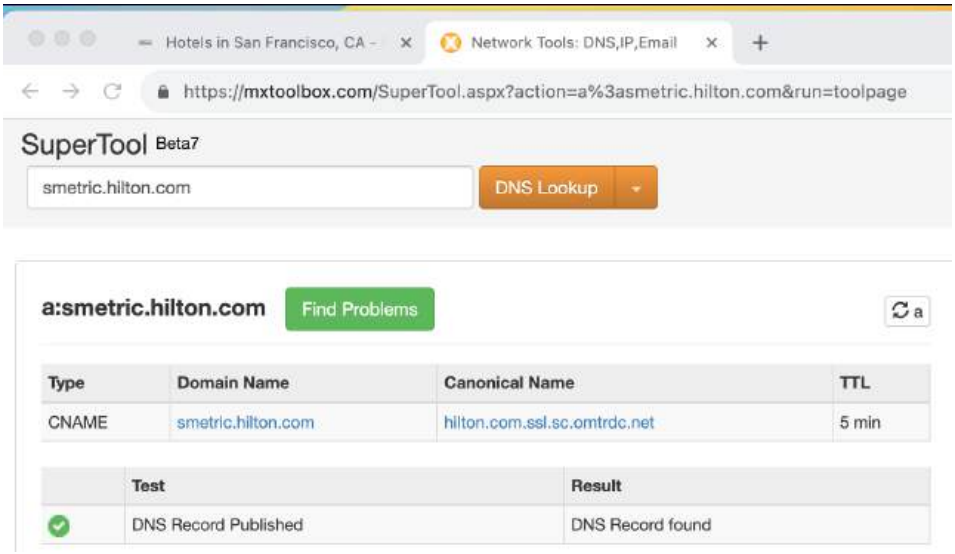
[13] Shared Data Under Measurement Controller-Controller Data Protection Terms (available at https://support.google.com/analytics/answer/9024351).

[14] *See, e.g.,* Adobe Experience League: Adobe Analytics cookies (available at https://experienceleague.adobe.com/en/docs/core-services/interface/data-collection/cookies/analytics); *see also* Adobe Experience League: Audience Manager cookies (available at https://experienceleague.adobe.com/en/docs/core-services/interface/data-collection/cookies/audience-manager).

[15] *See, e.g.,* Adobe Audience Manager User Guide: Data Collection Components (available at https://experienceleague.adobe.com/en/docs/audience-manager/user-guide/reference/system-components/components-data-collection).

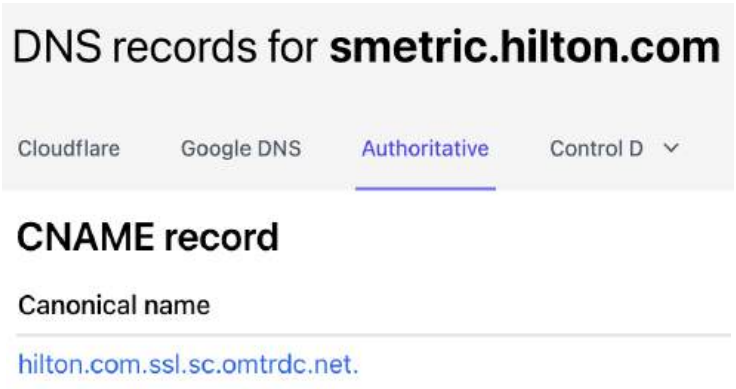
51. Adobe aggregates this cookie data with other data from multiple channels and devices, including web analytics, CRM systems, and e-commerce platforms, to create consumer profiles containing detailed information about a consumer's behavior, preferences, and demographics, create audience segments based on shared traits (such as millennials, tech enthusiasts, etc.), and to enable targeted advertising and marketing analytics.[16]

52. Defendant has configured a subdomain it owns and operates, at smetric.hilton.com, to point directly to Adobe's endpoint, at hilton.com.ssl.sc.omtrdc.net:[17]



[16] *See, e.g.*, Adobe Audience Manager User Guide: Understanding Calls to the Demdex Domain (available at https://experienceleague.adobe.com/en/docs/audience-manager/user-guide/reference/demdex-calls); Adobe Experience Cloud Identity Service overview (available at https://experienceleague.adobe.com/en/docs/id-service/using/intro/overview); Adobe Audience Manager Features (available at https://business.adobe.com/products/audience-manager/features.html); *see also* Audience Manager Overview (available at https://experienceleague.adobe.com/en/docs/audience-manager/user-guide/overview/aam-overview).

[17] Data obtained from https://mxtoolbox.com and https://www.nslookup.io/



53. The omtrdc.net domain is owned and operated by Adobe, and functions as a tracking server for Adobe Analytics.[18]

54. For example, when a user searches for hotels in San Francisco, the website causes the following type of data to be sent to Adobe Analytics at hilton.com.ssl.sc.omtrdc.net, via the smetric.hilton.com subdomain:

Request Header Query Body Cookies Raw Summary +

Key	Value
AQB	1
ndh	1
pf	1
callback	s_c_il[1].doPostbacks
et	1
t	7%2F9%2F2023%2013%3A38%3A46%206%20420
d.	
nsid	0
jsonv	1
.d	
mid	41702232992936575562205778250591185886
aamlh	9
ce	UTF-8
pageName	Browser%3AEN%3AMultibrand%3ACategoryPage%3ALocations%3AUS%7CCA%3ASan%20Francisco

[18] *See* https://experienceleague.adobe.com/en/docs/target/using/integrate/a4t/analytics-tracking-server

g	https%3A%2F%2Fwww.hilton.com%2Fen%2Flocations%2Fusa%2Fcalifornia%2Fsan-francisco%2F%3FdatelessMvtChoice%3Db
cc	USD
events	event119
v27	Browser%3AEN%3AMultibrand%3ACategoryPage%3ALocations%3AUS%7CCA%3ASan%20Francisco
v59	multibrand
pe	lnk_o
pev2	AWS%20Chat%20-%20Chat%20Presented
s	2240x1260
c	30
j	1.6
v	N
k	Y
bw	649
bh	987
mcorgid	F0C120B3534685700A490D45%40AdobeOrg
lrt	315
AQE	1

55. The "mid" parameter is Adobe's unique user identifier that persists across sessions, used to identify a visitor in the Adobe ecosystem.[19]

56. The "pageName" and "g" parameters correspond to the name of the page and url that the user is browsing. In this case, the values of the parameters contain the user's search string ("San Francisco"), revealing to Adobe that the user was searching for hotels in San Francisco.

57. Along with this data, the Adobe software code that Defendant causes to be stored on and executed by the user's device causes the following cookies to be sent to Adobe:

[19] *See* https://experienceleague.adobe.com/en/docs/analytics/components/metrics/unique-visitors

Request Header Query Body Cookies Raw Summary +

Key	Value
__lt__cid.47135154	86f46223-bb9d-4fd5-9e17-20f4b07c5533
__lt__sid.47135154	0b20ae9e-910e4a98
_abck	55FE5653E1A96C4359D0AC4CE3BAACE8~0~YAAQl/TVFw1kLvWKAQAAAXfbCwo8JYBslulZfIsJAHUL7H+6noU4skI2A/7+R2g0Ps5y3DEgOzbZkGMZMeFWg6tiGO1qetwbYDdnXV/b/qj1Y4JXOkRpTJLAxqkE2lGiR1VcmYoJArzy/UgiYLVi8ojQqaBAJYmR+V+v6qJmxMzMwqm8gMMMOBAg5wwCCt7R3Lk5OXxTmQHoAUifKCVMWiMDhvmGl7gpGQciSyr6TAi9fGfbxr+xOUjl8X5lkyi8KE/9BknZ4g0b//GBuvgZZL4C4veXWLusW2VjZFFIj+nkV+mxUdgKzKjyer3Eg0glRJyc5LqrkbKTprSnOcm+l60+bx9ijn8qtGGLcRHwG3ywGT0MdTv+F1Sp3mQSF4ib9kBaNncQnTm0VF2fEozYKdgdZC8uNmYOK3hUCjX8lXmE9at4Rc0HiBhzCGmIjkPDe032wp+Gm9J/~-1~-1~1696714567
_fbp	fb.1.1696711017940.1438213681
_gcl_au	1.1.1648324264.1696711019
_pin_unauth	dWlkPVptWmxaakkzWmpFdE1tUmpZeTAwT1dGaExUazBZV0l0WldFek5tWXlPV1ZsWmpkag
_scid	5b9e5461-f48f-45c6-836e-1a10256b2b4f
_scid_r	5b9e5461-f48f-45c6-836e-1a10256b2b4f
_sctr	1%7C1696662000000
_uetsid	42436670655111ee86b3339bdb3d083b
_uetvid	42436300655111ee9aaf836fc1ac976a
aam_uuid	41678662076505314832203624045623958161
ak_bmsc	EC63D9FE7F41756E8D1A3D8A9F647B39~000000000000000000000000000000~YAAQl/TVF/hjLvWKAQAAonbbCxXugb33S9EyRd13hpfIyWaTb5KKA0pGQmqaoWkT/mOmIeEhMdVBNdSyAMzUoPEiRjvv3N+f0dCzd0u5F+OGLBkKsaRKVvx4ADPaE2NkCWK18j/NQnOtjp/SE8nbqA6/ACPMK9/nGSOWnv6losrkH+398eD7vgxeq5CXSEmpdjybv5q5lRvkJhWKlbeu9pyBklKWK1WAj0zbb0qaTqAL8C7bT+B48BRQs7YvPaU6JZMg2tXFVYSNoF+6jCoW8Mpt8y5OJqueHSHQKiRODqpcXfg7/g4pBMaSRoBUDKZeimoxvrNpIYSKcaOECaTYXoxFN0P6vsDqnOOcZTUx5Kda+nXgspgtA3FfwmKtPY6eyuJrhlg5PkSikQ==
AKA_A2	A
AMCV_F0C120B3534685700A490D45%40AdobeOrg	179643557%7CMCIDTS%7C19638%7CMCMID%7C41702232992936575562205778250591185886%7CMCAAMLH-1697315816%7C9%7CMCAAMB-1697315816%7CRKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y%7CMCOPTOUT-1696718216s%7CNONE%7CMCAID%7CNONE%7CvVersion%7C5.5.0
AMCVS_F0C120B3534685700A490D45%40AdobeOrg	1
bm_sv	D0BFA4AAE349223367052DC00ADEF1C0~YAAQm/TVF4Q0pgCLAQAAWSzdCxX1jEdwkg4Yu5wUpEC7cy+5TCw+zWxkb1Eod9MPSvUgyoNeZvQZnqRJXuLA3NxojcM6j8KXSEbdYL97B43lt0rT7emqS9LWzW5qRD1n5Wexf2UmfJgrfx/WgnJQug8OQAGh2yNtlq8SBPJX7Vfo9Mmbqo3rguc1IfUq72tE/dNawtnWdGKivl/bAKOVPz6REL5T46SPuLprFwrgsj56YPOU0xbjKSeQBi3oLut8~1
bm_sz	CC4D379CE9706CEA61F79A2F876F9AFE~YAAQl/TVF8ZiLvWKAQAANnDbCxXsZm8bKlyoWju9dcHTLEsOJMHv3+LsJfSzhVUMIxwzYZGfz4MGtHKDL6cWQOn+fEXvmWuYAyVDUOR4L69QU0kenEdUg6o6t3Mxomc43CepsfLAJ7xhrWW3z+zOgbl6+T5FdBEy/emrbQPpgpx/r/fyge+lW0G1ilNU+LcN1E8wBbdWUTlJLuMYPO4Dm3U9ilbCifQBgrlEpLN8XfZrAdTF+Ll6+coew5dVkqlMhZbUQxB3CaSIITMRq6zK+N1FFU6XkX41OkNbuKGmBJOYmeg=~4403777~3687223
cmapi_cookie_privacy	permit 1 required
cmapi_gtm_bl	ga-ms-ua-ta-asp-bzi-sp-awct-cts-csm-img-flc-fls-mpm-mpr-m6d-tc-tdc
dtCookie	v_4_srv_3_sn_LB7U36ABIP71KV2HH5AITGDS0E4A2LFG_app-3A0da30f11c94bda74_1_ol_0_perc_100000_mul_1_rcs-3Acss_0
dtPC	3$511123880_920h16vQQTLWTRTRLPPOMGUUAHFPTAFHUFMKHCV-0e0
dtSa	-
fltk	segID%3D15195757

forterToken	5f65946e5744421c9e4d5f4226592a0f_1696711124332__UDF43-m4_15ck
ftr_blst_1h	1696711016504
gpv_v9	Browser%3AEN%3AMultibrand%3ACategoryPage%3ALocations%3AUS%7CCA%3ASan%20Francisco
notice_behavior	implied,us
notice_gdpr_prefs	0:
notice_preferences	0:
RT	"z=1&dm=hilton.com&si=a35c06aa-f5b9-4725-9ffe-2d615a847068&ss=lnghxfgy&sl=2&se=p0&tt=7tk&bcn=%2F%2F17de4c15.akstat.io%2F"
rxVisitor	16967110125660MT443UVP6CVUFVIJ7O9PDDOAKHPM22U
rxvt	1696712926006|1696711012567
s_cc	true
s_ecid	MCMID%7C41702232992936575562205778250591185886
s_sq	%5B%5BB%5D%5D
TAsessionID	c4e474ef-81c3-4e5b-8413-fb50ed31bbae|NEW
TMS	web%3D17836315%2Cweb-app%3D15195757%2Cweb-app%3D16416847%2CWeb-app%3D17146407%2Cweb-app%3D17347117%2Cweb-app%3D17567317%2Cweb-app%3D17727890%2Cweb-app%3D19484989%2Cweb-app%3D21881915

58. According to Adobe documentation, the cookies beginning with "AMCV_..." and "AMCVS_..." are tracking cookies, enabling Adobe to identify the unique user and to track them across other Adobe-integrated websites.[20]

59. The "s_ecid" cookie is used to store the Experience Cloud ID (ECID) or MID, further enabling Adobe to track the user.[21]

60. In addition, because of the way Defendant has configured its smetric.hilton.com subdomain, a large number of non-Adobe cookies are sent to Adobe, including cookies typically used by Microsoft Ads, Google Ads, Facebook, Pinterest, and Snap. For example, the "_fbp" cookie above is a Facebook cookie, and can be used to identify the user's Facebook account.

61. Further, along with all of this data, the Adobe software code that Defendant causes to be stored on and executed by the user's device causes the user's "user-agent" information to be sent to Adobe:

[20] See https://experienceleague.adobe.com/en/docs/id-service/using/intro/cookies

[21] See https://experienceleague.adobe.com/en/docs/core-services/interface/data-collection/cookies/analytics

Key	Value
user-agent	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36

As discussed above with respect to Google, the "user-agent" corresponds to the device and browser that the user has used to access the Website. In this example, the user-agent value corresponds to Google's Chrome browser version 121, running on the Catalina version of macOS.[22]

62. Finally, the data sent to Adobe includes the user's IP address.

3. Additional Cookies

63. Defendant also causes third party cookies to be transmitted to and from Website users' browsers and devices, even after users elect to opt out of all cookies, to and from other domains, including bat.bing.com and tr.snapchat.com.

64. The **bat.bing.com** domain is associated with associated with Bing, Microsoft's search engine, as well as Microsoft's digital advertising and analytics platforms. When a webpage loads a bat.bing.com cookie, it "tells Microsoft Advertising about the user visits to [the] webpage."[23] Microsoft uses bat.bing.com cookies to "record[] what customers do on [a] website and send[] that information to Microsoft Advertising." [24]

65. Bat.bing.com cookies collect consumers' (i) search history and browsing history, (ii) visit history, (iii) website interactions, (iv) user input data, (v) demographic information (including zip code[25]; gender[26]; age[27] (including identifying whether that person is a minor or

[22] There are many tools on the web that are capable of parsing user-agent strings to determine what browser and operating system they pertain to. One such tool is located at https://explore.whatismybrowser.com/useragents/parse.

[23] Microsoft Advertising Help: Everything you need to know about setting up UET (available at https://help.ads.microsoft.com/apex/index/3/en/56959#:~:text=The%20most%20important%20request%20is,making%20when%20your%20webpage%20loads).

[24] Microsoft Advertising Help: What is UET and how can it help me? (available at https://help.ads.microsoft.com/#apex/ads/en/56960/1).

[25] Microsoft Advertising Help: Legal, privacy, and personalization (available at https://help.ads.microsoft.com/#apex/ads/en/60212/0).

[26] *Id.*

[27] *Id.*

not)); (vi) interests and preferences, (vii) shopping behaviors, (viii) device information, (ix) referring URLs, (x) session information, (xi) user identifiers, and (xii) geolocation data (including IP addresses). Microsoft updates this information each time a user clicks on a website hosting a third-party bat.bing.com cookie.

66. Bat.bing.com cookies help Microsoft track users' interactions with ads (e.g., clicking a link or making a purchase) and provide valuable metrics that advertisers use to measure ad campaign performance. Further, bat.bing.com cookies allow Microsoft to obtain and store at user data to "help [website owners] focus a campaign or ad group on potential audiences who meet [website owners'] specific criteria, so [website owners] can increase the chance that [consumers] see [website owners'] ads." [28] Further, bat.bing.com cookies offer valuable "conversion tracking," which is a "measure [of] the ROI (return on investment) of your advertising campaign by letting [website owners] assign a monetary value to the activities people complete on [their] website after clicking [website owners'] ad."[29]

67. Microsoft also utilizes bat.bing.com data for its own purposes, including by using the data to tailor content and target advertisements to users. This profile enables Microsoft to deliver highly targeted ads within Microsoft's extensive advertising network Microsoft's revenue from its advertising network program has exceeded $10 billion as of 2022.[30]

68. The subdomain **tr.snapchat.com** is associated with Snap Inc. (SnapChat), a social media company that uses its cookies to measure users' conduct across distinct websites to help advertisers target ads.[31] SnapChat uses tr.snapchat.com to collect data on browsing history,

[28] *Id.*

[29] Microsoft Advertising Help: What is conversion tracking? (available at https://help.ads.microsoft.com/#apex/ads/en/56680/2).

[30] Microsoft's ad revenue hit $10B, and it's investing — is it a sleeping giant about to wake? (Ronan Shields) January 27, 2022 (available at https://digiday.com/media/microsofts-ad-revenue-hit-10b-and-its-investing-is-a-sleeping-giant-about-to-wake/).

[31] *See* https://snapdiscoveries.com/what-is-tr-snapchat-com-is-used-for.

choices, and interactions with advertisements.[32] This data helps Snapchat personalize ad content and track users across the internet.[33]

69. These cookies allow these Third Parties to obtain and store at least the following user data: (i) browsing history, (ii) visit history, (iii) website interactions, (iv) demographic information, (v) interests and preferences, (vi) shopping behaviors, (vii) device information, (viii) referring URLs, (ix) session information, (x) user identifiers, and/or (xi) geolocation data.

E. The Private Communications Collected are Valuable.

70. The Personal Communications that the Third Parties track and collect by way of the cookies on the Website are valuable to Defendant as well as the Third Parties. Defendant can use the data to create and analyze the performance of marketing campaigns, website design, product placement, and target specific users or groups of users for advertisements. For instance, if Defendant wanted to market certain of its hotel and resorts to consumers, Defendant could use the data collected by the Third Parties to monitor users who visit webpages related to specific products, then advertise similar products to those particular users when they visit other webpages. The third-party cookies also enable Defendant to target online advertisements to users when they visit ***other*** websites, even those completely unrelated to Defendant and its products.

71. Data about users' browsing history enables Defendant to spot patterns in users' behavior on the Website and their interests in, among other things, Defendant's hotel and resorts. On a broader scale, it enables Defendant to gain an understanding of trends happening across its brands and across the hospitality market. All of this helps Defendant further monetize its Website and maximize revenue by collecting and analyzing user data.

72. The value of the Private Communications tracked and collected by the Third Parties using cookies on the Website can be quantified. Legal scholars observe that "[p]ersonal information is an important currency in the new millennium."[34] Indeed, "[t]he monetary value

[32] *Id.*

[33] *Id.*

[34] *See* Paul M. Schwartz, *Property, Privacy and Personal Data*, 117 Harv. L. Rev. 2055, 2056–57 (2004).

of personal data is large and still growing, and corporate America is moving quickly to profit from the trend." *Id*. "Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information." *Id*.

73. Numerous empirical studies quantify the appropriate value measure for personal data. Generally, the value of personal data is measured as either the consumer's willingness to accept compensation to sell her data or the consumer's willingness to pay to protect her information.

74. Through its false representations and aiding, agreeing with, employing, permitting, or otherwise enabling the Third Parties to track users' Private Communications on the Website using third-party cookies, Defendant is unjustly enriching itself at the cost of consumer privacy and choice, when the consumer could otherwise have the ability to choose if and how they would monetize their data.

PLAINTIFFS' EXPERIENCES

Plaintiff Shah

75. In or around March 2023, Plaintiff Shah visited the Website to browse information about Hilton's hotels and resorts.

76. When Plaintiff Shah visited the Website, the Website immediately presented him with Defendant's popup cookie consent banner, which provided the option to select the "Opt Out" button. Plaintiff Shah viewed Defendant's representation on the popup cookie consent banner that, "We use cookies and similar technologies to provide you with personalized content, improve site performance, and conduct analytics. We also work with third parties to show you content and advertisements for products and services you might like. These third parties use cookies on this site to process your personal data for their own purposes. If you wish to opt out of cookies and similar technologies, please click the Opt Out button." Plaintiff Shah also viewed Defendant's additional representation that users could "Opt Out" of cookies by clicking the button.

77. Consistent with his typical practice in rejecting or otherwise opting out of the placement or use of cookies and tracking technologies, Plaintiff Shah selected and clicked the

"Opt Out" button. Plaintiff Shah believed that selecting the "Opt Out" button on the popup cookie consent banner found on the Website would allow him to opt out of, decline, and/or reject all cookies and other tracking technologies (inclusive of those cookies that cause the disclosure of user data to third-parties for the purposes of providing personalized content, advertising, and analytics services).

78. In selecting the "Opt Out" button, Plaintiff Shah gave Defendant notice that he did not consent to the use or placement of cookies and tracking technologies while browsing the Website. Further, Plaintiff Shah specifically opted out of or rejected, based on Defendant's representations, those cookies used to "personalize[] content, improve site performance, and conduct analytics … [and] advertisements" and share users' "personal data" with third parties. In reliance on these representations and promises, only then did Plaintiff Shah continue browsing the Website.

79. Even before the popup cookie consent banner appeared on the screen, Defendant nonetheless caused cookies and tracking technologies, including those used for personalized content, advertising, and analytics, to be placed on Plaintiff Shah's device and/or transmitted to the Third Parties along with user data, without Plaintiff Shah's knowledge. Accordingly, the popup cookie consent banner's representation to Plaintiff Shah that he could opt out of or reject the use and/or placement of cookies and tracking technologies while he browsed the Website was false. Contrary to what Defendant made Plaintiff Shah believe, he did not have a choice about whether third-party cookies would be placed on his device and/or transmitted to the Third Parties along with his user data; rather, Defendant had already caused that to happen.

80. Then, as Plaintiff Shah continued to browse the Website in reliance on the promises Defendant made in the cookie consent banner, and despite Plaintiff Shah's clear rejection of the use and/or placement of such cookies and tracking technologies, Defendant nonetheless continued to cause the placement and/or transmission of cookies along with user data, including those involved in providing personalized content, advertising, and analytics from

the Third Parties on his device. In doing so, Defendant permitted the Third Parties to track and collect Plaintiff Shah's Private Communications as Plaintiff Shah browsed the Website.

81. Defendant's representations that consumers could "Opt Out" of cookies while Plaintiff Shah and users browsed the Website, or at least those involved in providing personalized content, advertising, and analytics services, were untrue. Had Plaintiff Shah known this fact, he would not have used the Website. Moreover, Plaintiff Shah reviewed the popup cookie consent banner and Privacy Statement prior to using the Website. Had Defendant disclosed that it would continue to cause cookies and tracking technologies to be stored on consumers' devices even after they choose to reject cookies, Plaintiff Shah would have noticed it and would not have used the Website or, at a minimum, he would have interacted with the Website differently.

82. Plaintiff Shah continues to desire to browse content featured on the Website. Plaintiff Shah would like to browse websites that do not misrepresent that users can opt out of or reject cookies and tracking technologies. If the Website were programmed to honor users' requests to opt out of cookies and tracking technologies, Plaintiff Shah would likely browse the Website again in the future, but will not do so until then. Plaintiff Shah regularly visits websites that feature content similar to that of the Website. Because Plaintiff Shah does not know how the Website is programmed, which can change over time, and because he does not have the technical knowledge necessary to test whether the Website honors users' requests to opt out of cookies and tracking technologies, Plaintiff Shah will be unable to rely on Defendant's representations when browsing the Website in the future absent an injunction that prohibits Defendant from making misrepresentations on the Website. The only way to determine what network traffic is sent to third parties when visiting a website is to use a specialized tool such as Chrome Developer Tools. As the name suggests, such tools are designed for use by "developers" (i.e., software developers), whose specialized training enables them to analyze the data underlying the HTTP traffic to determine what data, if any, is being sent to whom. Plaintiff Shah is not a software developer and has not received training with respect to HTTP network calls.

Plaintiff Gabrielli

83. In or around August 2024 and November 2024, Plaintiff Gabrielli visited the Website to browse information about Hilton's hotels and resorts.

84. When Plaintiff Gabrielli visited the Website, the Website immediately presented him with Defendant's popup cookie consent banner, which provided the option to select the "Opt Out" button. Plaintiff Gabrielli viewed Defendant's representation on the popup cookie consent banner that, "We use cookies and similar technologies to provide you with personalized content, improve site performance, and conduct analytics. We also work with third parties to show you content and advertisements for products and services you might like. These third parties use cookies on this site to process your personal data for their own purposes. If you wish to opt out of cookies and similar technologies, please click the Opt Out button." Plaintiff Gabrielli also viewed Defendant's additional representation that users could "Opt Out" of cookies by clicking the button.

85. Consistent with his typical practice in rejecting or otherwise opting out of the placement or use of cookies and tracking technologies, Plaintiff Gabrielli selected and clicked the "Opt Out" button. Plaintiff Gabrielli believed that selecting the "Opt Out" button on the popup cookie consent banner found on the Website would allow him to opt out of, decline, and/or reject all cookies and other tracking technologies (inclusive of those cookies that cause the disclosure of user data to third-parties for the purposes of providing personalized content, advertising, and analytics services).

86. In selecting the "Opt Out" button, Plaintiff Gabrielli gave Defendant notice that he did not consent to the use or placement of cookies and tracking technologies while browsing the Website. Further, Plaintiff Gabrielli specifically opted out of or rejected, based on Defendant's representations, those cookies used to "personalize[] content, improve site performance, and conduct analytics … [and] advertisements" and share users' "personal data" with third parties. In reliance on these representations and promises, only then did Plaintiff Gabrielli continue browsing the Website.

87. Even before the popup cookie consent banner appeared on the screen, Defendant nonetheless caused cookies and tracking technologies, including those used for personalized content, advertising, and analytics, to be placed on Plaintiff Gabrielli's device and/or transmitted to the Third Parties along with user data, without Plaintiff Gabrielli's knowledge. Accordingly, the popup cookie consent banner's representation to Plaintiff Gabrielli that he could opt out of or reject the use and/or placement of cookies and tracking technologies while he browsed the Website was false. Contrary to what Defendant made Plaintiff Gabrielli believe, he did not have a choice about whether third-party cookies would be placed on his device and/or transmitted to the Third Parties along with his user data; rather, Defendant had already caused that to happen.

88. Then, as Plaintiff Gabrielli continued to browse the Website in reliance on the promises Defendant made in the cookie consent banner, and despite Plaintiff Gabrielli's clear rejection of the use and/or placement of such cookies and tracking technologies, Defendant nonetheless continued to cause the placement and/or transmission of cookies along with user data, including those involved in providing personalized content, advertising, and analytics from the Third Parties on his device. In doing so, Defendant permitted the Third Parties to track and collect Plaintiff Gabrielli's Private Communications as Plaintiff Gabrielli browsed the Website.

89. Defendant's representations that consumers could "Opt Out" of cookies while Plaintiff Gabrielli and users browsed the Website, or at least those involved in providing personalized content, advertising, and analytics services, were untrue. Had Plaintiff Gabrielli known this fact, he would not have used the Website. Moreover, Plaintiff Gabrielli reviewed the popup cookie consent banner and Privacy Statement prior to using the Website. Had Defendant disclosed that it would continue to cause cookies and tracking technologies to be stored on consumers' devices even after they choose to reject cookies, Plaintiff Gabrielli would have noticed it and would not have used the Website or, at a minimum, he would have interacted with the Website differently.

90. Plaintiff Gabrielli continues to desire to browse content featured on the Website. Plaintiff Gabrielli would like to browse websites that do not misrepresent that users can opt out

of or reject cookies and tracking technologies. If the Website were programmed to honor users' requests to opt out of cookies and tracking technologies, Plaintiff Gabrielli would likely browse the Website again in the future, but will not do so until then. Plaintiff Gabrielli regularly visits websites that feature content similar to that of the Website. Because Plaintiff Gabrielli does not know how the Website is programmed, which can change over time, and because he does not have the technical knowledge necessary to test whether the Website honors users' requests to opt out of cookies and tracking technologies, Plaintiff Gabrielli will be unable to rely on Defendant's representations when browsing the Website in the future absent an injunction that prohibits Defendant from making misrepresentations on the Website. The only way to determine what network traffic is sent to third parties when visiting a website is to use a specialized tool such as Chrome Developer Tools. As the name suggests, such tools are designed for use by "developers" (i.e., software developers), whose specialized training enables them to analyze the data underlying the HTTP traffic to determine what data, if any, is being sent to whom. Plaintiff Gabrielli is not a software developer and has not received training with respect to HTTP network calls.

Plaintiff Wiley

91. In or around spring 2023 and July 2024, Plaintiff Wiley visited the Website to browse information about Hilton's hotels and resorts.

92. When Plaintiff Wiley visited the Website, the Website immediately presented her with Defendant's popup cookie consent banner, which provided the option to select the "Opt Out" button. Plaintiff Wiley viewed Defendant's representation on the popup cookie consent banner that, "We use cookies and similar technologies to provide you with personalized content, improve site performance, and conduct analytics. We also work with third parties to show you content and advertisements for products and services you might like. These third parties use cookies on this site to process your personal data for their own purposes. If you wish to opt out of cookies and similar technologies, please click the Opt Out button." Plaintiff Wiley also viewed

Defendant's additional representation that users could "Opt Out" of cookies by clicking the button.

93. Consistent with her typical practice in rejecting or otherwise opting out of the placement or use of cookies and tracking technologies, Plaintiff Wiley selected and clicked the "Opt Out" button. Plaintiff Wiley believed that selecting the "Opt Out" button on the popup cookie consent banner found on the Website would allow her to opt out of, decline, and/or reject all cookies and other tracking technologies (inclusive of those cookies that cause the disclosure of user data to third-parties for the purposes of providing personalized content, advertising, and analytics services).

94. In selecting the "Opt Out" button, Plaintiff Wiley gave Defendant notice that she did not consent to the use or placement of cookies and tracking technologies while browsing the Website. Further, Plaintiff Wiley specifically opted out of or rejected, based on Defendant's representations, those cookies used to "personalize[] content, improve site performance, and conduct analytics … [and] advertisements" and share users' "personal data" with third parties. In reliance on these representations and promises, only then did Plaintiff Wiley continue browsing the Website.

95. Even before the popup cookie consent banner appeared on the screen, Defendant nonetheless caused cookies and tracking technologies, including those used for personalized content, advertising, and analytics, to be placed on Plaintiff Wiley's device and/or transmitted to the Third Parties along with user data, without Plaintiff Wiley's knowledge. Accordingly, the popup cookie consent banner's representation to Plaintiff Wiley that she could opt out of or reject the use and/or placement of cookies and tracking technologies while she browsed the Website was false. Contrary to what Defendant made Plaintiff Wiley believe, she did not have a choice about whether third-party cookies would be placed on her device and/or transmitted to the Third Parties along with her user data; rather, Defendant had already caused that to happen.

96. Then, as Plaintiff Wiley continued to browse the Website in reliance on the promises Defendant made in the cookie consent banner, and despite Plaintiff Wiley's clear

rejection of the use and/or placement of such cookies and tracking technologies, Defendant nonetheless continued to cause the placement and/or transmission of cookies along with user data, including those involved in providing personalized content, advertising, and analytics from the Third Parties on her device. In doing so, Defendant permitted the Third Parties to track and collect Plaintiff Wiley's Private Communications as Plaintiff Wiley browsed the Website.

97. Defendant's representations that consumers could "Opt Out" of cookies while Plaintiff Wiley and users browsed the Website, or at least those involved in providing personalized content, advertising, and analytics services, were untrue. Had Plaintiff Wiley known this fact, she would not have used the Website. Moreover, Plaintiff Wiley reviewed the popup cookie consent banner and Privacy Statement prior to using the Website. Had Defendant disclosed that it would continue to cause cookies and tracking technologies to be stored on consumers' devices even after they choose to reject cookies, Plaintiff Wiley would have noticed it and would not have used the Website or, at a minimum, she would have interacted with the Website differently.

98. Plaintiff Wiley continues to desire to browse content featured on the Website. Plaintiff Wiley would like to browse websites that do not misrepresent that users can opt out of or reject cookies and tracking technologies. If the Website were programmed to honor users' requests to opt out of cookies and tracking technologies, Plaintiff Wiley would likely browse the Website again in the future, but will not do so until then. Plaintiff Wiley regularly visits websites that feature content similar to that of the Website. Because Plaintiff Wiley does not know how the Website is programmed, which can change over time, and because she does not have the technical knowledge necessary to test whether the Website honors users' requests to opt out of cookies and tracking technologies, Plaintiff Wiley will be unable to rely on Defendant's representations when browsing the Website in the future absent an injunction that prohibits Defendant from making misrepresentations on the Website. The only way to determine what network traffic is sent to third parties when visiting a website is to use a specialized tool such as Chrome Developer Tools. As the name suggests, such tools are designed for use by "developers"

(i.e., software developers), whose specialized training enables them to analyze the data underlying the HTTP traffic to determine what data, if any, is being sent to whom. Plaintiff Wiley is not a software developer and has not received training with respect to HTTP network calls.

TOLLING

99. All applicable statutes of limitations have been tolled by operation of the delayed discovery doctrine, which delays accrual until Plaintiffs have, or should have, inquiry notice of their causes of action. Despite exercising reasonable diligence, Plaintiffs were unaware of Defendant's fraudulent and unlawful conduct alleged herein due to Defendant's active concealment of material facts, which prevented Plaintiffs from discovering their claims within the statute of limitations. As alleged above, Plaintiffs do not have the expertise to test whether the Website honored users' requests to opt out of cookies and tracking technologies. Plaintiffs were unaware that even though they opted out of cookies on the Website, Defendant caused cookies, including the Third Parties' cookies, to be sent to their browsers, stored on their devices, and transmitted to the Third Parties along with private user data until on or around January 2025 when they learned of Defendant's privacy violations from counsel.

100. On or around October 14, 2023, Defendant was notified of the claims and allegations asserted herein. Defendant was not prejudiced in its ability to gather evidence for Plaintiffs' claims since the claims asserted herein are substantially similar to those raised in the October 14, 2023 letter.

CLASS ALLEGATIONS

101. Plaintiffs bring this Class Action Complaint on behalf of themselves and a proposed class of similarly situated persons, pursuant to Rules 23(b)(2) and (b)(3) of the Federal Rules of Civil Procedure. Plaintiffs seek to represent the following group of similarly situated persons, defined as follows:

Class: All persons who browsed the Website in the State of California after clicking the "Opt Out" button in the popup cookies consent banner within the four years preceding the filing of this Complaint (the "Class Period").

102. This action has been brought and may properly be maintained as a class action against Defendant because there is a well-defined community of interest in the litigation and the proposed class is easily ascertainable.

103. **Numerosity:** Plaintiffs do not know the exact size of the Class, but they estimate that it is composed of more than 100 persons. The persons in the Class are so numerous that the joinder of all such persons is impracticable and the disposition of their claims in a class action rather than in individual actions will benefit the parties and the courts.

104. **Common Questions Predominate:** This action involves common questions of law and fact to the Class because each class member's claim derives from the same unlawful conduct that led them to believe that Defendant would not cause third-party cookies to be placed on their browsers and devices and/or transmitted to third parties along with user data, after Class members chose to opt out of or reject cookies and tracking technologies on the Website, nor would Defendant permit third parties to track and collect Class members' Private Communications as Class members browsed the Website.

105. The common questions of law and fact predominate over individual questions, as proof of a common or single set of facts will establish the right of each member of the Class to recover. The questions of law and fact common to the Class are:

a. Whether Defendant's actions violate California laws invoked herein; and

b. Whether Plaintiffs and Class members are entitled to damages, restitution, injunctive and other equitable relief, reasonable attorneys' fees, prejudgment interest and costs of this suit.

106. **Typicality:** Plaintiffs' claims are typical of the claims of the other members of the Class because, among other things, Plaintiffs, like the other Class members, visited the Website, opted out of cookies, and had their confidential Private Communications intercepted by the Third Parties.

107. **Adequacy of Representation:** Plaintiffs will fairly and adequately protect the interests of all Class members because it is in their best interests to prosecute the claims alleged herein to obtain full compensation due to them for the unfair and illegal conduct of which they complain. Plaintiffs also have no interests in conflict with, or antagonistic to, the interests of Class members. Plaintiffs have retained highly competent and experienced class action attorneys to represent their interests and those of the Class. By prevailing on their claims, Plaintiffs will establish Defendant's liability to all Class members. Plaintiffs and their counsel have the necessary financial resources to adequately and vigorously litigate this class action, and Plaintiffs and counsel are aware of their fiduciary responsibilities to the Class members and are determined to diligently discharge those duties by vigorously seeking the maximum possible recovery for Class members.

108. **Superiority:** There is no plain, speedy, or adequate remedy other than by maintenance of this class action. The prosecution of individual remedies by members of the Class will tend to establish inconsistent standards of conduct for Defendant and result in the impairment of Class members' rights and the disposition of their interests through actions to which they were not parties. Class action treatment will permit a large number of similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of effort and expense that numerous individual actions would engender. Furthermore, as the damages suffered by each individual member of the Class may be relatively small, the expenses and burden of individual litigation would make it difficult or impossible for individual members of the class to redress the wrongs done to them, while an important public interest will be served by addressing the matter as a class action. Plaintiffs are unaware of any difficulties that are likely to be encountered in the management of this action that would preclude its maintenance as a class action.

CAUSES OF ACTION

First Cause of Action: Invasion of Privacy

109. Plaintiffs reallege and incorporate the paragraphs of this Complaint as if set forth herein.

110. To plead a California constitutional privacy claim, Plaintiffs must show an invasion of (i) a legally protected privacy interest; (ii) where Plaintiffs had a reasonable expectation of privacy in the circumstances; and (iii) conduct by Defendant constituting a serious invasion of privacy.

111. Defendant has intruded upon the following legally protected privacy interests of Plaintiffs and Class members: (i) the California Invasion of Privacy Act, as alleged herein; (ii) the California Constitution, which guarantees Californians the right to privacy; (iii) the California Wiretap Acts as alleged herein; (iv) Cal. Penal Code § 484(a), which prohibits the knowing theft or defrauding of property "by any false or fraudulent representation or pretense;" and (v) Plaintiffs' and Class members' Fourth Amendment right to privacy.

112. Plaintiffs and Class members had a reasonable expectation of privacy under the circumstances, as Defendant affirmatively promised users they could "Opt Out" of cookies and tracking technologies before proceeding to browse the Website. Plaintiffs and other Class members directed their electronic devices to access the Website and, when presented with the popup cookies consent banner on the Website, Plaintiffs and Class members opted out of or rejected cookies and reasonably expected that their rejection of cookies and tracking technologies would be honored. That is, they reasonably believed that Defendant would not permit the Third Parties to store and send cookies and/or use other such tracking technologies on their devices while they browsed the Website. Plaintiffs and Class members also reasonably expected that, if they opted out of such cookies and/or tracking technologies, Defendant would not permit the Third Parties to track and collect Plaintiffs' and Class members' Private Communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device

information, referring URLs, session information, user identifiers, and/or geolocation data, on the Website.

113. Such information is "personal information" under California law, which defines personal information as including "Internet or other electronic network activity information," such as "browsing history, search history, and information regarding a consumer's interaction with an internet website, application, or advertisement." Cal. Civ. Code § 1798.140.

114. Defendant, in violation of Plaintiffs' and other Class members' reasonable expectation of privacy and without their consent, permits the Third Parties to use cookies and other tracking technologies to collect, track, and compile users' Private Communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data. The data that Defendant allowed third parties to collect enables the Third Parties to, *inter alia*, create consumer profiles containing detailed information about a consumer's behavior, preferences, and demographics; create audience segments based on shared traits (such as millennials, tech enthusiasts, etc.); and perform targeted advertising and marketing analytics. Further, the Third Parties share user data and/or the user profiles to unknown parties to further their financial gain. The consumer profiles are and can be used to further invade Plaintiffs' and users' privacy, by allowing third parties to learn intimate details of their lives, and target them for advertising and other purposes, as described herein, thereby harming them through the abrogation of their autonomy and their ability to control dissemination and use of information about them.

115. Defendant's actions constituted a serious invasion of privacy in that it invaded a zone of privacy protected by the Fourth Amendment (i.e., one's personal communications), and violated criminal laws on wiretapping and invasion of privacy. These acts constitute an egregious breach of social norms that is highly offensive.

116. Defendant's intrusion into Plaintiffs' privacy was also highly offensive to a reasonable person.

117. Defendant lacked a legitimate business interest in causing the placement and/or transmission of third-party cookies along with user data that allowed the Third Parties to track, intercept, receive, and collect Private Communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data, without their consent.

118. Plaintiffs and Class members have been damaged by Defendant's invasion of their privacy and are entitled to just compensation, including monetary damages.

119. Plaintiffs and Class members seek appropriate relief for that injury, including but not limited to, damages that will compensate them for the harm to their privacy interests as well as disgorgement of profits made by Defendant as a result of its intrusions upon Plaintiffs' and Class members' privacy.

120. Plaintiffs and Class members seek punitive damages because Defendant's actions—which were malicious, oppressive, willful—were calculated to injure Plaintiffs and Class members and made in conscious disregard of Plaintiffs' and Class members' rights and Plaintiffs' and Class members' opt out of the Website's use of cookies. Punitive damages are warranted to deter Defendant from engaging in future misconduct.

Second Cause of Action: Intrusion Upon Seclusion

121. Plaintiffs reallege and incorporate by reference all paragraphs alleged herein.

122. To assert a claim for intrusion upon seclusion, Plaintiffs must plead (i) that Defendant intentionally intruded into a place, conversation, or matter as to which Plaintiffs had a reasonable expectation of privacy; and (ii) that the intrusion was highly offensive to a reasonable person.

123. By permitting third-party cookies to be stored on consumers' devices, which enabled the Third Parties to track and collect Plaintiffs' and Class members' Private Communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device

information, referring URLs, session information, user identifiers, and/or geolocation data, in violation of Defendant's representations otherwise in the popup cookie consent banner, Defendant intentionally intruded upon the solitude or seclusion of Website users. Defendant effectively placed the Third Parties in the middle of communications to which they were not invited, welcomed, or authorized.

124. The Third Parties' tracking and collecting of Plaintiffs' and Class member's Private Communications on the Website using third-party cookies that Defendant caused to be stored on users' devices—and to be transmitted to Third Parties—was not authorized by Plaintiffs and Class members, and, in fact, those Website users specifically chose to "Opt Out" of cookies.

125. Plaintiffs and the Class members had an objectively reasonable expectation of privacy surrounding their Private Communications on the Website based on Defendant's promise that users could "Opt Out" of cookies, as well as state criminal and civil laws designed to protect individual privacy.

126. Defendant's intentional intrusion into Plaintiffs' and other users' Private Communications would be highly offensive to a reasonable person given that Defendant represented that Website users could "Opt Out"of cookies when, in fact, Defendant caused such third-party cookies to be stored on consumers' devices and browsers, and to be transmitted to third parties, even when consumers opted out of or rejected all such cookies. Indeed, Plaintiffs and Class members reasonably expected, based on Defendant's false representations, that when they opted out of cookies and tracking technologies, Defendant would not cause such third-party cookies to be stored on their devices or permit the Third Parties to obtain their Private Communications on the Website, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data.

127. Defendant's conduct was intentional and intruded on Plaintiffs' and users' Private Communications on the Website.

128. Plaintiffs and Class members have been damaged by Defendant's invasion of their privacy and are entitled to just compensation, including monetary damages.

129. Plaintiffs and Class members seeks appropriate relief for that injury, including but not limited to, damages that will compensate them for the harm to their privacy interests as well as disgorgement of profits made by Defendant as a result of its intrusions upon Plaintiffs' and Class members' privacy.

130. Plaintiffs and Class members seek punitive damages because Defendant's actions—which were malicious, oppressive, willful—were calculated to injure Plaintiffs and Class members and made in conscious disregard of Plaintiffs' and Class members' rights and Plaintiffs' and Class members' opt out of and rejection of the Website's use of cookies. Punitive damages are warranted to deter Defendant from engaging in future misconduct.

Third Cause of Action: Wiretapping in Violation of the California Invasion of Privacy Act (California Penal Code § 631)

131. Plaintiffs reallege and incorporate by reference all paragraphs alleged herein.

132. California Penal Code § 631(a) provides, in pertinent part:

> "Any person who, by means of any machine, instrument, or contrivance, or in any other manner . . . willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars . . . ."

133. The California Supreme Court has repeatedly stated an "express objective" of CIPA is to "protect a person placing or receiving a call from a situation where the person on the other end of the line permits an outsider to tap his telephone or listen in on the call." *Ribas v. Clark*, 38 Cal. 3d 355, 364 (1985) (emphasis added).

134. Further, as the California Supreme Court has held, in explaining the legislative purpose behind CIPA:

> While one who imparts private information risks the betrayal of his confidence by the other party, a substantial distinction has been recognized between the secondhand repetition of the contents of a conversation and *its simultaneous dissemination to an unannounced second auditor, whether that auditor be a person or mechanical device.*
>
> As one commentator has noted, such secret monitoring denies the speaker an important aspect of privacy of communication— the right to control the nature and extent of the firsthand dissemination of his statements.

Ribas, 38 Cal. 3d at 360-61 (emphasis supplied; internal citations omitted).

135. CIPA § 631(a) imposes liability for "distinct and mutually independent patterns of conduct." *Tavernetti v. Superior Ct.*, 22 Cal. 3d 187, 192-93 (1978). Thus, to establish liability under § 631(a), Plaintiffs need only establish that Defendant, "by means of any machine, instrument, contrivance, or in any other manner," did ***any*** of the following:

> [i] Intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system;
>
> [ii] Willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read or learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable or is being sent from or received at any place within this state;
>
> [iii] Uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained

Cal. Penal Code § 631(a).

136. CIPA § 631(a) also penalizes those who [iv] "aid[], agree[] with, employ[], or conspire[] with any person" who conducts the aforementioned wiretapping, or those who "permit" the wiretapping.

137. Defendant is a "person" within the meaning of California Penal Code § 631.

138. Section 631(a) is not limited to phone lines, but also applies to "new technologies" such as computers, the Internet, and email. *See Matera v. Google Inc.*, 2016 WL 8200619, at *21 (N.D. Cal. Aug. 12, 2016) (CIPA applies to "new technologies" and must be

construed broadly to effectuate its remedial purpose of protecting privacy); *see also Bradley v. Google, Inc.*, 2006 WL 3798134, at *5–6 (N.D. Cal. Dec. 22, 2006) (CIPA governs "electronic communications"); *Javier v. Assurance IQ, LLC*, 2022 WL 1744107, at *1 (9th Cir. May 31, 2022) ("Though written in terms of wiretapping, Section 631(a) applies to Internet communications.").

139. The Third Parties' cookies—as well as the software code of the Third Parties responsible for placing the cookies and transmitting data from user devices to the Third Parties—constitute "machine[s], instrument[s], or contrivance[s]" under the CIPA (and, even if they do not, Defendant's deliberate and purposeful scheme that facilitated the interceptions falls under the broad statutory catch-all category of "any other manner").

140. Each of the Third Parties is a "separate legal entity that offers [a] 'software-as-a-service' and not merely a passive device." *Saleh v. Nike, Inc.*, 562 F. Supp. 3d 503, 520 (C.D. Cal. 2021). Further, the Third Parties had the capability to use the wiretapped information for their own purposes and, as alleged above, they did in fact use the wiretapped information for their own business purposes. Accordingly, the Third Parties were third parties to any communication between Plaintiffs and Class members, on the one hand, and Defendant, on the other. *Id.* at 521; *see also Javier v. Assurance IQ, LLC*, 649 F. Supp. 3d 891, 900 (N.D. Cal. 2023).

141. Under § 631(a), Defendant must show it had the consent of all parties to a communication.

142. At all relevant times, the Website caused Plaintiffs' and Class members' browsers to store the Third Parties' cookies and to transmit those cookies alongside Private Communications—including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data—to the Third Parties without Plaintiff's and Class members' consent. By configuring the Website in this manner, Defendant willfully aided, agreed with, employed, permitted, or otherwise enabled

the Third Parties to wiretap Plaintiffs and Class members using the Third Parties' cookies and to accomplish the wrongful conduct alleged herein.

143. At all relevant times, by their cookies and corresponding software code, the Third Parties willfully and without the consent of all parties to the communication, or in any unauthorized manner, read, attempted to read, and/or learned the contents or meaning of electronic communications of Plaintiffs and Class members, on the one hand, and Defendant, on the other, while the electronic communications were in transit or were being sent from or received at any place within California.

144. The Private Communications of Plaintiffs and Class members, on the one hand, and Defendant, on the other, that the Third Parties automatically intercepted directly communicates the Website user's affirmative decisions, actions, choices, preferences, and activities, which constitute the "contents" of electronic communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data.

145. At all relevant times, the Third Parties used or attempted to use the Private Communications automatically intercepted by their cookie tracking technologies for their own purposes.

146. Plaintiffs and Class members did not provide their prior consent to the Third Parties' intentional access, interception, reading, learning, recording, collection, and usage of Plaintiffs' and Class members' electronic communications. Nor did Plaintiffs and Class members provide their prior consent to Defendant aiding, agreeing with, employing, permitting, or otherwise enabling the Third Parties' conduct. On the contrary, Plaintiffs and Class members expressly declined to allow Third Parties' cookies and tracking technologies to access, intercept, read, learn, record, collect, and use Plaintiffs' and Class members' electronic communications by choosing to opt out of cookies in the consent banner.

147. The wiretapping of Plaintiffs and Class members occurred in California, where Plaintiffs and Class members accessed the Website and where the Third Parties—as enabled by Defendant—routed Plaintiffs' and Class members' electronic communications to Third Parties' servers. Among other things, the cookies, as well as the software code responsible for placing the cookies and transmitting them and other Private Communications to the Third Parties, resided on Plaintiffs' California-located devices. In particular, the user's California-based device, after downloading the software code from the Third Parties' servers, (i) stored the code onto the user's disk; (ii) converted the code into machine-executable format; and (iii) executed the code, causing the transmission of data (including cookie data) to and from the Third Parties.

148. Plaintiffs and Class members have suffered loss by reason of these violations, including, but not limited to, (i) violation of their right to privacy; (ii) loss of value in their Private Communications; (iii) damage to and loss of Plaintiff's and Class members' property right to control the dissemination and use of their Private Communications; and (iv) loss of their Private Communications to the Third Parties with no consent.

149. Pursuant to California Penal Code § 637.2, Plaintiffs and Class members have been injured by the violations of California Penal Code § 631, and each seeks statutory damages of the greater of $5,000, or three times the amount of actual damages, for each of Defendant's violations of CIPA § 631(a), as well as injunctive relief.

150. Unless enjoined, Defendant will continue to commit the illegal acts alleged herein including, but not limited to, permitting third parties to access, intercept, read, learn, record, collect, and use Plaintiffs' and Class members' electronic Private Communications with Defendant. Plaintiffs, Class members, and the general public continue to be at risk because Plaintiffs, Class members, and the general public frequently use the internet to search for information and content related to its hotels and resorts. Plaintiffs, Class members, and the general public continue to desire to use the internet for that purpose. Plaintiffs, Class members, and the general public have no practical way to know if their request to opt out of cookies and tracking technologies will be honored and/or whether Defendant will permit third parties to

access, intercept, read, learn, record, collect, and use Plaintiffs' and Class members' electronic Private Communications with Defendant. Further, Defendant has already permitted the Third Parties to access, intercept, read, learn, record, collect, and use Plaintiffs' and Class members' electronic Private Communications with Defendant and will continue to do so unless and until enjoined.

Fourth Cause of Action: Use of a Pen Register in Violation of the California Invasion of Privacy Act (California Penal Code § 638.51)

151. Plaintiffs reallege and incorporate by reference all paragraphs alleged herein.

152. The California Invasion of Privacy Act, codified at Cal. Penal Code §§ 630 to 638, includes the following statement of purpose:

> The Legislature hereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.

153. California Penal Code Section 638.51(a) proscribes any "person" from "install[ing] or us[ing] a pen register or a trap and trace device without first obtaining a court order."

154. A "pen register" is a "a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication." Cal. Penal Code § 638.50(b).

155. The Third Parties' cookies and the corresponding software code installed by Defendant on its Website are each "pen registers" because they are "device[s] or process[es]" that "capture[d]" the "routing, addressing, or signaling information"—including, the IP address and user-agent information—from the electronic communications transmitted by Plaintiffs' and the Class's computers or devices. Cal. Penal Code § 638.50(b).

156. At all relevant times, Defendant caused the Third Parties' cookies and the corresponding software code—which are pen registers—to be placed on Plaintiffs' and Class

members' browsers and devices, and/or to be used to transmit Plaintiffs' and Class members' IP address and user-agent information. *See Greenley v. Kochava,* 2023 WL 4833466, at *15-16 (S.D. Cal. July 27, 2023); *Shah v. Fandom, Inc.*, 2024 U.S. Dist. LEXIS 193032, at *5-11 (N.D. Cal. Oct. 21, 2024).

157. Some of the information collected by the Third Parties' cookies and the corresponding software, including IP addresses and user-agent information, does not constitute the content of Plaintiffs' and the Class's electronic communications with the Website. *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1008 (9th Cir. 2014). ("IP addresses constitute addressing information and do not necessarily reveal any more about the underlying contents of communication…") (cleaned up).

158. Plaintiffs and Class members did not provide their prior consent to Defendant's use of third-party cookies and the corresponding software. On the contrary, Plaintiffs and the Class members informed Defendant that they did not consent to the Website's use of third-party cookies by clicking the "Opt Out" button in the cookie consent banner.

159. Defendant did not obtain a court order to install or use the third-party cookies and the corresponding software to track and collect Plaintiffs' and Class member's IP addresses and user-agent information.

160. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class members suffered losses and were damaged in an amount to be determined at trial.

161. Pursuant to Penal Code § 637.2(a)(1), Plaintiffs and Class members are also entitled to statutory damages of $5,000 for each of Defendant's violations of § 638.51(a).

Fifth Cause of Action: Common Law Fraud, Deceit and/or Misrepresentation

162. Plaintiffs reallege and incorporate by reference all paragraphs alleged herein.

163. Defendant fraudulently and deceptively informed Plaintiffs and Class members that they could "Opt Out" of cookies.

164. However, despite Defendant's representations otherwise, Defendant caused third-party cookies and software code to be stored on consumers' devices, and to be transmitted to the

Third Parties alongside Private Communications, even after users clicked the "Opt Out" button in the popup cookie consent banner. These cookies and corresponding software code allowed the Third Parties to access, intercept, read, learn, record, collect, and use Plaintiffs' and Class members' Private Communications, even when consumers had previously chosen to "Opt Out" of cookies.

165. These misrepresentations and omissions were known exclusively to, and actively concealed by Defendant, not reasonably known to Plaintiffs and Class members, and material at the time they were made. Defendant knew, or should have known, how the Website functioned, including the Third Party's resources it installed on the Website and the third-party cookies in use on the Website, through testing the Website, evaluating its performance metrics by means of its accounts with the Third Parties, or otherwise, and knew, or should have known, that the Website's programming allowed the third-party cookies to be placed on users'—including Plaintiffs'—browsers and devices and/or transmitted to the Third Parties along with users' Private Communications even after users attempted to "Opt Out" of cookies, which Defendant promised its users they could do. Defendant's misrepresentations and omissions concerned material facts that were essential to the analysis undertaken by Plaintiffs and Class members as to whether to use the Website. In misleading Plaintiffs and Class members and not so informing them, Defendant breached its duty to Plaintiffs and Class members. Defendant also gained financially from, and as a result of, its breach.

166. Plaintiffs and Class members relied to their detriment on Defendant's misrepresentations and fraudulent omissions.

167. Plaintiffs and Class members have suffered an injury-in-fact, including the loss of money and/or property, as a result of Defendant's unfair, deceptive, and/or unlawful practices, including the unauthorized interception of their Personal Communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data, which have value as demonstrated by the

use and sale of consumers' browsing activity, as alleged above. Plaintiffs and Class members have also suffered harm in the form of diminution of the value of their private and personally identifiable information and communications.

168. Defendant's actions caused damage to and loss of Plaintiffs' and Class members' property right to control the dissemination and use of their personal information and communications.

169. Defendant's representation that consumers could opt out of cookies (including "cookies and similar technologies to provide you with personalized content, improve site performance, and conduct analytics … [and] advertisements") if they clicked the "Opt Out" button was untrue. Again, had Plaintiffs and Class members known these facts, they would not have used the Website. Moreover, Plaintiffs and Class members reviewed the popup cookie consent banner and Privacy Statement prior to their interactions with the Website. Had Defendant disclosed that it caused third-party cookies to be stored on Website visitors' devices that are related to personalization, advertising, and analytics and/or share information with third parties even after they choose to opt out of all such cookies, Plaintiffs and Class members would have noticed it and would not have interacted with the Website.

170. By and through such fraud, deceit, misrepresentations and/or omissions, Defendant intended to induce Plaintiffs and Class members to alter their positions to their detriment. Specifically, Defendant fraudulently and deceptively induced Plaintiffs and Class members to, without limitation, use the Website under the mistaken belief that Defendant would not permit third parties to obtain users' Private Communications when consumers chose to opt out of cookies. As a result, Plaintiff and the Class provided more personal data than they would have otherwise.

171. Plaintiffs and Class members justifiably and reasonably relied on Defendant's misrepresentations and omissions, and, accordingly, were damaged by Defendant's conduct.

172. As a direct and proximate result of Defendant's misrepresentations and/or omissions, Plaintiffs and Class members have suffered damages, as alleged above, and are entitled to just compensation, including monetary damages.

173. Plaintiffs and Class members seek punitive damages because Defendant's actions—which were malicious, oppressive, willful—were calculated to injure Plaintiffs and Class members and made in conscious disregard of Plaintiffs' and Class members' rights and Plaintiffs' and Class members' opt out of and rejection of the Website's use of cookies. Punitive damages are warranted to deter Defendant from engaging in future misconduct.

Sixth Cause of Action: Unjust Enrichment

174. Plaintiffs reallege and incorporate by reference all paragraphs alleged herein.

175. Defendant created and implemented a scheme to increase its own profits through a pervasive pattern of false statements and fraudulent omissions.

176. Defendant was unjustly enriched as a result of its wrongful conduct, including through its misrepresentation that users could "Opt Out" of cookies and by permitting the Third Parties to store and transmit cookies on Plaintiffs' and Class members' devices and browsers, which permitted the Third Parties to track and collect users' Private Communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data, even after Class members opted out of such cookies.

177. Plaintiffs and Class members' Personal Communications have conferred an economic benefit on Defendant.

178. Defendant has been unjustly enriched at the expense of Plaintiffs and Class members, and Defendant has unjustly retained the benefits of its unlawful and wrongful conduct.

179. Defendant appreciated, recognized, and chose to accept the monetary benefits that Plaintiffs and Class members conferred onto Defendant at their detriment. These benefits were

the expected result of Defendant acting in its pecuniary interest at the expense of Plaintiffs and Class members.

180. It would be unjust for Defendant to retain the value of Plaintiffs' and Class members' property and any profits earned thereon.

181. There is no justification for Defendant's enrichment. It would be inequitable, unconscionable, and unjust for Defendant to be permitted to retain these benefits because the benefits were procured as a result of its wrongful conduct.

182. Plaintiffs and Class members are entitled to restitution of the benefits Defendant unjustly retained and/or any amounts necessary to return Plaintiffs and Class members to the position they occupied prior to having their Private Communications tracked and collected by the Third Parties.

183. Plaintiffs plead this claim separately, as well as in the alternative, to their other claims, as without such claims Plaintiffs would have no adequate legal remedy.

Seventh Cause of Action: Breach of Contract

184. Plaintiffs reallege and incorporate by reference all paragraphs alleged herein.

185. Defendant's relationship with its users is governed by the Website's Privacy Statement, which explains:

> Hilton's mission is to be the most hospitable company in the world. We're passionate about delivering exceptional guest experiences, and we look forward to welcoming you to our hotels so we can share the light and warmth of hospitality with you.
>
> We pledge to deliver the highest level of customer service, which includes respecting your privacy and protecting your personal information. In this privacy statement ("Statement"), we provide you with details about how we collect, use, and disclose your personal information.
>
> This Statement applies to Hilton Worldwide Holdings Inc., its subsidiaries, and all of the hotels within the Hilton Portfolio of Brands (collectively, "Hilton," "we," or "us"). Our Portfolio of Brands includes Waldorf Astoria Hotels & Resorts, LXR Hotels & Resorts, Conrad Hotels & Resorts, Canopy by Hilton, Signia by Hilton, Hilton Hotels & Resorts, Curio Collection by Hilton, DoubleTree by Hilton, Tapestry Collection by Hilton, Embassy Suites by Hilton, Tempo by Hilton, Motto by Hilton, Hilton Garden Inn, Hampton by Hilton, Tru by Hilton, Homewood Suites by Hilton, and Home2 Suites by Hilton.

> By using any of our products or services and/or by agreeing to this Statement, e.g. in the context of registering for any of our products or services, you understand and acknowledge that we will collect and use personal information as described in this Statement.

186. The Website's Privacy Statement contains enforceable promises that Defendant made to Plaintiffs and Class members, including, but not limited to, the following provision:

> If you would like to opt out of the sale of your personal information, you may do so by clicking on the banner that appears on any Hilton website when you access that site from an IP address that relates to California or by visiting our website at datarights.hilton.com or click the "Personal Data Requests" link at the bottom of any Hilton website to submit your request. Please note that when you opt out of cookies, tags, and pixels, that opt out only pertains to the device and the browser that you are using when you opt out. If you wish to opt out for other devices or browsers, you must opt out again when you are using those devices or browsers.

187. Defendant breached these duties and violated these promises by causing third-party cookies to be stored on consumers' devices and browsers that enabled the Third Parties to track and collect Plaintiffs' and Class member's Private Communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data, even though Defendant represented that Plaintiffs and other users could "Opt Out" of cookies. Plaintiffs and Class members, in fact, chose to opt out of such cookies by selecting the "Opt Out" button.

188. At all relevant times and in all relevant ways, Plaintiffs and Class members performed their obligations under the Privacy Statement or were excused from performance of such obligations through the unknown and unforeseen conduct of others.

189. Defendant's conduct in permitting the Third Parties to track and collect the Private Communications of Website users who chose to reject all cookies and tracking technologies evaded the spirit of the bargain made between Defendant and Plaintiff and Class members since it caused Plaintiff and Class members to surrender more data than they had otherwise bargained for.

190. As a direct and proximate result of Defendant's breach of contract, Plaintiffs and Class members did not receive the full benefit of the bargain, and instead received services from Defendant that were less valuable than described in the Privacy Statement. Plaintiffs and Class members, therefore, were damaged in an amount at least equal to the difference in value between that which was promised and Defendant's partial, deficient, and/or defective performance.

191. As a direct consequence of the breaches of contract and violations of promises described above, Plaintiffs and Class members seek nominal damages, general damages, compensatory damages, consequential damages, unjust enrichment, and any other just relief.

Eighth Cause of Action: Breach of Implied Covenant of Good Faith and Fair Dealing

192. Plaintiffs reallege and incorporate by reference all paragraphs alleged herein.

193. Defendant's relationship with its users is governed by the Website's Privacy Statement, which explains:

> Hilton's mission is to be the most hospitable company in the world. We're passionate about delivering exceptional guest experiences, and we look forward to welcoming you to our hotels so we can share the light and warmth of hospitality with you.
>
> We pledge to deliver the highest level of customer service, which includes respecting your privacy and protecting your personal information. In this privacy statement ("Statement"), we provide you with details about how we collect, use, and disclose your personal information.
>
> This Statement applies to Hilton Worldwide Holdings Inc., its subsidiaries, and all of the hotels within the Hilton Portfolio of Brands (collectively, "Hilton," "we," or "us"). Our Portfolio of Brands includes Waldorf Astoria Hotels & Resorts, LXR Hotels & Resorts, Conrad Hotels & Resorts, Canopy by Hilton, Signia by Hilton, Hilton Hotels & Resorts, Curio Collection by Hilton, DoubleTree by Hilton, Tapestry Collection by Hilton, Embassy Suites by Hilton, Tempo by Hilton, Motto by Hilton, Hilton Garden Inn, Hampton by Hilton, Tru by Hilton, Homewood Suites by Hilton, and Home2 Suites by Hilton.
>
> By using any of our products or services and/or by agreeing to this Statement, e.g. in the context of registering for any of our products or services, you understand and acknowledge that we will collect and use personal information as described in this Statement.

194. The Website's Privacy Statement contains enforceable promises that Defendant made to Plaintiffs and Class members, including, but not limited to, the following provision:

> If you would like to opt out of the sale of your personal information, you may do so by clicking on the banner that appears on any Hilton website when you access that site from an IP address that relates to California or by visiting our website at datarights.hilton.com or click the "Personal Data Requests" link at the bottom of any Hilton website to submit your request. Please note that when you opt out of cookies, tags, and pixels, that opt out only pertains to the device and the browser that you are using when you opt out. If you wish to opt out for other devices or browsers, you must opt out again when you are using those devices or browsers.

195. Defendant breached these duties and violated these promises by causing third-party cookies to be stored on consumers' devices and browsers that enabled the Third Parties to track and collect Plaintiffs' and Class member's Private Communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data, even though Defendant represented that Plaintiffs and other users could opt out of cookies and tracking technologies. Plaintiffs and Class members, in fact, chose to opt out of such cookies by selecting the "Opt Out" button. California law recognizes the implied covenant of good faith and fair dealing in every contract.

196. In dealing between Defendant and its Website users, Defendant is invested with discretionary power affecting the rights of its users.

197. Defendant purports to respect and protect its Website users' privacy.

198. Despite their contractual promises to allow consumers to opt out of cookies and other tracking technologies, Defendant took actions outside that contractual promise to deprive consumers, including Plaintiffs and other users similarly situated, of benefits of their contract with Defendant.

199. Defendant's allowance of third parties to track and collect Website users' Private Communications with Defendant was objectively unreasonable given its privacy promises.

200. Defendant's conduct in permitting third parties to track and collect the Private Communications of Website users who chose to opt out of cookies and tracking technologies

evaded the spirit of the bargain made between Defendant and Plaintiffs and Class members since it caused Plaintiffs and Class members to surrender more data than they had otherwise bargained for.

201. As a result of Defendant's misconduct and breach of its duty of good faith and fair dealing, Plaintiffs and Class members suffered damages. Plaintiffs and Class members did not receive the benefit of the bargain for which they contracted and for which they paid valuable consideration in the form of providing their personal information, which, as alleged above, has ascertainable value.

202. As a direct consequence of the breach of the implied covenant of good faith and fair dealing described above, Plaintiffs and Class members seek nominal damages, general damages, compensatory damages, consequential damages, and any other just relief.

Ninth Cause of Action: Trespass to Chattels

203. Plaintiffs reallege and incorporate by reference all paragraphs alleged herein.

204. Defendant, intentionally and without consent or other legal justification, caused cookies to be stored on Plaintiffs' and Class members' browsers and devices, which enabled the Third Parties and Defendant to track and collect Plaintiffs' and Class members' Private Communications and use the data collected for their own advantage, as described above.

205. Defendant was unjustly enriched as a result of its wrongful conduct, including through its misrepresentation that users could opt out of cookies and tracking technologies, and through their failure to disclose that Defendant causes third-party cookies to be stored on consumers' devices and browsers, which cause the Third Parties and Defendant to track and collect Plaintiffs' and Class members' Private Communications even after consumers chose to opt out of or reject such cookies.

206. Defendant intentionally caused third party software code to be stored onto Plaintiffs' and Class members' devices, knowing that the code would be executed by those devices. The software code then placed and/or transmitted cookies along with Plaintiffs' and Class members' Private Communications to the Third Parties. These intentional acts interfered

with Plaintiffs' and Class members' use of the following personal property owned, leased, or controlled by Plaintiffs and other users: (a) her and their computers and other electronic devices; and (b) her and their personally identifiable information.

207. Defendant's trespass of Plaintiffs' and other users' computing devices resulted in harm to Plaintiffs and other users and caused Plaintiffs and other users the following damages:

a. Nominal damages for trespass;

b. Reduction of storage, disk space, and performance of Plaintiffs' and Class members' computing devices; and

c. Loss of value of Plaintiffs' and Class members' computing devices.

PRAYER FOR RELIEF

WHEREFORE, reserving all rights, Plaintiffs, on behalf of themselves and the Class members, respectfully request judgment against Defendant as follows:

A. Certification of the proposed Class, including appointment of Plaintiffs' counsel as class counsel;

B. An award of compensatory damages, including statutory damages where available, to Plaintiffs and Class members against Defendant for all damages sustained as a result of Defendant's wrongdoing, including both pre- and post-judgment interest thereon;

C. An award of punitive damages;

D. An award of nominal damages;

E. An order for full restitution;

F. An order requiring Defendant to disgorge revenues and profits wrongfully obtained;

G. An order temporarily and permanently enjoining Defendant from continuing the unlawful, deceptive, fraudulent, and unfair business practices alleged in this Complaint;

H. For reasonable attorneys' fees and the costs of suit incurred; and

I. For such further relief as may be just and proper.

Dated: January 31, 2025

GUTRIDE SAFIER LLP

/s/ Seth A. Safier
Seth A. Safier (State Bar No. 197427)
seth@gutridesafier.com
Marie A. McCrary (State Bar No. 262670)
marie@gutridesafier.com
Todd Kennedy (State Bar No. 250267)
todd@gutridesafier.com
Kali R. Backer (State Bar No. 342492)
kali@gutridesafier.com
100 Pine Street, Suite 1250
San Francisco, CA 94111
Telephone: (415) 639-9090
Facsimile: (415) 449-6469

Attorneys for Plaintiff